

PRINCIPIO DI BON ORDINAMENTO

Sia \mathbb{N} l'insieme degli interi non negativi $\{0, 1, 2, \dots\}$
e $S \subseteq \mathbb{N}$. Se $S \neq \emptyset \Rightarrow S$ ha un elemento minimo

PRINCIPIO DI INDUZIONE

Sia $S \subseteq \mathbb{N}$ con le seguenti proprietà:

i) $0 \in S$

ii) $n \in S \Rightarrow n+1 \in S$

Allora $S = \mathbb{N}$

PRINCIPIO DI INDUZIONE - FORMA COMPLETA

Sia $S \subseteq \mathbb{N}$ con le seguenti proprietà:

i) $0 \in S$

ii) $1, \dots, n \in S \Rightarrow n+1 \in S$

Allora $S = \mathbb{N}$

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

$a|b \Leftrightarrow \exists c \in \mathbb{Z}: ac = b$

DEF (mcm)

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

Allora $S = \{c \in \mathbb{N}^* = \{1, 2, \dots\} : a|c \wedge b|c\} \neq \emptyset$

perché $\pm ab \in S$.

L'elemento più piccolo di S è $\text{mcm}(a, b)$.

DIMOSTRAZIONE PER INDUZIONE

Sia $P(n)$ una proposizione $\forall n \in \mathbb{N}$.

Supponiamo che $P(0)$ vera e $P(k)$ vera $\Rightarrow P(k+1)$ vera

Allora $P(n)$ è vera $\forall n \in \mathbb{N}$.

DIM (TRAMITE PRINCIPIO DI BUON ORDINAMENTO)

Supponiamo $S = \{k \in \mathbb{N} : P(k) \text{ è falsa}\} \neq \emptyset$

Poiché $S \neq \emptyset$, S ha un elemento minimo s .

Per ipotesi $0 \notin S \Rightarrow s \geq 1 \Rightarrow s-1 \notin S$

$\Rightarrow P(s-1)$ è vera $\stackrel{\text{PER IPOTESI}}{\Rightarrow} P(s)$ è vera $\Rightarrow s \notin S \xrightarrow{\downarrow}$

$\Rightarrow S = \emptyset$ □

DIM (TRAMITE PRINCIPIO DI INDUZIONE)

Sia $S = \{k \in \mathbb{N} : P(k) \text{ è vera}\}$

Allora $0 \in S$ per ipotesi.

Per ipotesi $n \in S \Rightarrow n+1 \in S \Rightarrow S = \mathbb{N}$ □

DIMOSTRAZIONE PER INDUZIONE (FORTE)

Sia $P(n)$ una proposizione $\forall n \in \mathbb{N}$.

Supponiamo:

- $P(0)$ vera
- $P(0), \dots, P(k)$ vere $\Rightarrow P(k+1)$ vera

Allora $P(n)$ è vera $\forall n \in \mathbb{N}$

DIMOSTRAZIONE PER ASSURDO

Un modo per dimostrare che una proposizione P è vera è mostrare che assumere che $\neg P$ sia vero porta a una contraddizione.

Più precisamente, esiste una proposizione Q t.c.:

$$\neg P \Rightarrow Q \wedge (\neg Q) \text{ è vera}$$

Poiché $Q \wedge (\neg Q)$ è sempre falsa, ne segue che P è vera

DEF (NUMERO PRIMO)

Un numero primo p è un intero > 1 che non ha divisori interi positivi diversi da 1 e p

LEMMA Ogni intero > 1 ha un fattore primo

DIM

$P(2)$ è vera perché 2 è primo e soddisfa l'enunciato

Supponiamo che $P(2), P(3), \dots, P(n)$ siano vere

CASO 1: $n+1$ è primo

$P(n+1)$

CASO 2: $n+1$ non è primo

$a|n+1$ con $2 \leq a \leq n$

\Rightarrow / a è primo
OPPURE

✓ $p|a$ con p primi $\Rightarrow p|n+1 \Rightarrow n+1$ ha un fattore primo

TEOREMA DI EUCLIDE

Esistono infiniti numeri primi.

DIM

Sia $S = \{p \in \mathbb{N}^*: p \text{ è primo}\}$

Supponiamo $|S| < \infty$, allora $S = \{p_1, p_2, \dots, p_s\}$

Sia $m = p_1 \cdot p_2 \cdot \dots \cdot p_s$ il prodotto di tutti gli elem. di S .

Allora $p_j \nmid m+1 \forall j$

$\Rightarrow m+1$ è primo o ha un fattore primo $\notin S$ *

$\Rightarrow |S| = \infty$

□

TEOREMA DI DIVISIONE

Siamo $a \in \mathbb{N}^*$, $b \in \mathbb{N}$.

Allora esistono due interi $q \geq 0$ e $0 \leq r < a$ t.c. $b = qa + r$

DIM

Sia $S = \{b - ax \mid x \in \mathbb{N} \text{ e } b - ax \geq 0\}$

Allora $S \neq \emptyset$ perché $x=0 \Rightarrow b - ax = b \geq 0$

ordinamento

$\Rightarrow S$ ha un elemento minimo r (per il princ. del buon)

Per costruzione $r = b - qa$ con $q \geq 0$

Dobbiamo dimostrare $0 \leq r < a$.

Supponiamo per assurdo $r \geq a$.

Allora $r-a = b-q\alpha - a \geq 0$ che contraddice la minimalità
di $r \downarrow \uparrow$

$$\Rightarrow b = q\alpha + r \text{ con } 0 \leq r < a$$

□

PROPOSIZIONE (UNICITÀ DELLA COPPIA QUOTIENTE - RESTO)

Siamo $a \in \mathbb{N}^*$, $b \in \mathbb{N}$ e $b = q\alpha + r$ con $q \geq 0$ e $0 \leq r < a$

Allora la coppia (q, r) è unica

DIM

Supponiamo che (q', r') sia un'altra coppia t.c.

$$q' \geq 0 \text{ e } 0 \leq r' < a$$

Dopo avere eventualmente scambiato (q, r) e (q', r')

Supponiamo $r \geq r'$.

$$\text{Allora } 0 = b - b = q\alpha + r - (q'\alpha + r') = a(q-q') + (r-r')$$

$$\Rightarrow a(q'-q) = (r-r') \geq 0$$

$$\text{Ma } 0 \leq r' \leq r < a \Rightarrow 0 \leq (r-r') < a$$

$$\text{Dunque } q'-q = \frac{(r-r')}{a} \text{ con } 0 \leq \frac{(r-r')}{a} < 1 \Rightarrow q' = q$$

$$\Rightarrow r = b - q\alpha \quad | \\ r' = b - q'\alpha \quad | \quad q = q' \Rightarrow r = r'$$

□

DEF (QUOTIENTE E RESTO)

Siamo $a \in \mathbb{N}^*$, $b \in \mathbb{N}$ e $b = q\alpha + r$ con $q \geq 0$ e $0 \leq r < a$

Allora q è detto quoziente della divisione di b per a
e r è detto resto.

DEF (RAPPRESENTAZIONE IN BASE b)

Siamo $n \geq 0$ e $b \geq 2$ interi.

Allora, si dice che n ha una rappresentazione in base b se esiste una sequenza $\{a_0 \dots a_k\}$ t.c. $a_j \in \{0, \dots, b-1\} \forall j$ e $n = a_k b^k + \dots + a_1 b + a_0$.

La stringa " $a_k \dots a_0$ " è detta rappresentazione in base b di n .

TEOREMA (UNICITÀ DELLA RAPPRESENTAZIONE IN BASE b)

Fissato un intero $b \geq 2$, ogni intero $n \geq 0$ può essere rappresentato in base b : cioè n può essere scritto univocamente come $n = a_k b^k + \dots + a_1 b + a_0$ dove $a_j \in \{0, \dots, b-1\} \forall j = 0, \dots, k$

DIM

$P(n) = n$ ha una rappresentazione in base b

$P(0)$ vera

Supponiamo $P(0), \dots, P(k)$ vere

Allora $k+1 = bq + r$ con $0 \leq r < b$

Inoltre, poiché $b > 1 \Rightarrow q < k+1$

Per ipotesi: $q = q_m b^m + \dots + q_0$

$\Rightarrow k+1 = bq + r = b(q_m b^m + \dots + q_0) + r = q_m b^{m+1} + \dots + q_0 b + r$

è una rappre. di n in base b

Sia $S = \{ \text{int. non negativi che hanno una rappresentazione unica in base } b \}$

$S \neq \emptyset \Rightarrow S$ ha un elemento minimo n ($n \geq b$)

Siamo $n = a_k b^k + \dots + a_1 b + a_0$ e $n = c_l b^l + \dots + c_1 b + c_0$

due diverse rappre. di n in base b .

Allora $n = (a_k b^{k-1} + \dots + a_1) b + a_0 = Aq + a_0$ e $n = (c_l b^{l-1} + \dots + c_1) b + c_0 = Cq + c_0$

dove $0 \leq a_0 < b$ e $0 \leq c_0 < b$.

Per il th della divisione $a_0 = c_0 \Rightarrow A = C$ ha due diverse rappre. in base b . Ma $A < n$ *

□

ALGORITMO PER CALCOLARE LA RAPP. IN BASE b DI n

$$n = bq_0 + r_0, \quad q_0 = bq_1 + r_1, \dots q_k = b(0) + r_k$$

dove " $r_n r_{n-1} \dots r_0$ " è la rappr. di n in base b .

DEF (DI ELEM. MASSIMO)

Sia $S \subseteq \mathbb{R}$

Allora $m \in \mathbb{R}$ è un elemento massimo di S se:

- i) $m \in S$
- ii) $s \in S \Rightarrow s \leq m$

N.B.: in generale, un sottoinsieme di \mathbb{R} non deve necessariamente avere un elemento massimo.
Ad esempio, un sottoinsieme aperto di \mathbb{R} non ha mai un elemento max.

$$\text{ES: } (0,1) = \{x \in \mathbb{R} : 0 < x < 1\}$$

LEMMA (UNICITÀ DEL' ELEM. MASSIMO)

Sia $S \subseteq \mathbb{R}$.

Se S ha un elemento massimo m , allora S ha un unico elemento massimo.

DIM

Siano m, m' elementi massimi di S .

Allora $m \leq m'$ perché m' è max, ma anche $m' \leq m$ perché m è max.

$$\Rightarrow m = m'$$

□

In particolare questo deriva dalla proprietà antisimmetrica di una relazione d'ordine.

$$1) x \leq x \quad (\text{PROPRIETÀ RIFLESSIVA})$$

$$2) x \leq y, y \leq x \Rightarrow x = y \quad (\text{PROP. ANTISIMMETRICA})$$

$$3) x \leq y, y \leq z \Rightarrow x \leq z \quad (\text{PROP. TRANSITIVA})$$

LEMMA

Sia $S \subseteq \mathbb{N}$ finito, $S \neq \emptyset$.

Allora S ha un elemento massimo.

DIM

$P(n)$ = Se S ha $n \geq 1$ elementi, allora S ha un elem. max.

$P(1)$ vera (se S ha 1 solo elem., quell'elem. è il max)

Supponiamo che S abbia $n+1$ elementi.

$P(n)$ vera $\Rightarrow P(n+1)$ vera

Sia $r \in S \Rightarrow S' = S - \{r\}$ ha $n \geq 1$ elementi

$P(n)$ vera $\Rightarrow S'$ ha un elemento max r'

$\Rightarrow \max(r, r')$ è l'elemento max di S

□

Sia $n \in \mathbb{Z}$ e $D(n) = \{d \in \mathbb{Z} : d|n\}$. $D(0) = \mathbb{Z}$

PROPOSIZIONE

Sia n un intero diverso da zero.

Allora $D(n) \subseteq \{-|n|, \dots, |n|\}$

In particolare, $D(n)$ è un insieme finito.

DIM

$m \in D(n) \Rightarrow \exists k \in \mathbb{Z}$ t.c. $n = km$ con $k \neq 0$ e $m \neq 0$

perché $n \neq 0$.

Allora $|n| = |km| = |k||m| \Rightarrow |k|, |m| \leq |n|$

□

DEF (MCD)

Siamo a, b interi t.c. $(a, b) \neq (0, 0)$.

Il massimo comune divisore di a e b , $\text{MCD}(a, b)$ è il massimo dell'insieme $\underbrace{D(a) \cap D(b)}_{\text{DIVISORI DI } a}$.

N.B.: $\text{MCD}(0, b) = b$

$\text{MCD}(a, 0) = a$

$\text{MCD}(0, 0) = ?$ non è ben definito

La precedente definizione fornisce anche un algoritmo per calcolare $\text{MCD}(a, b)$:

```
int MCD ( int a, int b ) { // assumendo a, b > 0
    int k, m;
    for ( m = 1, k = 1, K = a + 1, k++ )
        if ( ( a % k ) == 0 && ( b % k ) == 0 ) m = k;
    return m;
}
```

LEMMA

Siamo a, b interi diversi da zero.

Allora $\text{MCD}(a+b, b) = \text{MCD}(a, b)$

DIM

Siamo $m = \text{MCD}(a+b, b)$ e $\mu = \text{MCD}(a, b)$

Allora:

$$m = \text{MCD}(a+b, b) \Rightarrow m | (a+b), m | b \Rightarrow m | a, m | b \Rightarrow m \leq \mu$$

Alllo stesso modo:

$$\mu = \text{MCD}(a, b) \Rightarrow \mu | a, \mu | b \Rightarrow \mu | (a+b), \mu | b \Rightarrow \mu \leq m$$
$$\Rightarrow m = \mu$$

□

Supponiamo $a \geq b > 0$ con $a = qb + r$ dove $0 \leq r < b$

Allora, il Lemma precedente implica:

$$\text{MCD}(a, b) = \text{MCD}(r+qb, b) = \text{MCD}(r, b) = \text{MCD}(b, r)$$

L'algoritmo termina quando $r = 0$.

In questo modo otteniamo un algoritmo per calc. MCD:

```
int MCD_Euclide ( int a, int b ) {
```

```
    if ( b == 0 ) return a;
```

```
    if ( b > a ) MCD ( b, a );
```

```
    return MCD ( b, a % b );
```

```
}
```

ALGORITMO DI EUCLIDE

La forma originale di questo algoritmo prevede che si applichi il th della divisione come segue:

$$b = aq_1 + r_1$$

$$a = r_1 q_2 + r_2$$

$$r_1 = r_2 q_3 + r_3$$

$$r_2 = r_3 q_4 + r_4$$

⋮

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

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

L'algoritmo termina quando r_n divide r_{n-1} .

A quel punto $r_n = \text{MCD}(a, b)$.

IDENTITÀ DI BEZOUT

Siamo a e b interi t.c. $(a, b) \neq (0, 0)$.

Sia $S = \{au + bv : u, v \in \mathbb{Z}\} \cap \mathbb{N}^*$

Allora $S \neq \emptyset$ perché $|a|, |b| \in S$.

Dunque S ha un elemento minimo $m = \text{MCD}(a, b)$.

DIM (che $m = \text{MCD}(a, b)$)

Mostriamo che $m | a$:

$$a = qm + r, \quad 0 \leq r < m, \quad m = au + bv$$

$$a = q(au + bv) + r \Rightarrow a - aqu - bv = a(1 - qu) - bv < m$$

Che contraddice la minimalità di m , a meno che $r = 0$.

$\Rightarrow m | a$ (allo stesso modo $m | b$)

Sia $\mu = \text{MCD}(a, b)$, allora $m \leq \mu$

Poiché $m = au + bv$ e $\mu | a, \mu | b \Rightarrow \mu | m \Rightarrow \mu = m$

□

IDENTITÀ DI BEZOUT

Se $a \neq b$ sono interi non nulli e $\text{MCD}(a,b) = d$, allora esistono due interi $u \neq v$ t.c. $d = au + bv$

LEMMA DI EUCLIDE

Un intero $p > 1$ è un numero primo se e solo se $p | ab \Rightarrow p | a \circ p | b \forall a, b$

DIM

Supponiamo p primo.

$$\text{MCD}(a, p) \neq 1 \Rightarrow p | a$$

$$\text{MCD}(b, p) \neq 1 \Rightarrow p | b$$

\Rightarrow dopo avere eventualmente scambiato a e b possiamo supporre $\text{MCD}(a, p) = 1$

Per l'identità di Bezout $\exists u, v$ t.c. $pu + bv = 1$

$$\Rightarrow b = b(pu + bv) = pbu + abv$$

Bidé, per ipotesi, $p | p$ e $p | ab \Rightarrow p | pbu + abv = b$

Se invece p non è primo $\exists a, b > 1$ t.c. $p = ab$

In particolare $p = ab$ e $a > 1 \Rightarrow b < p \Rightarrow p \nmid b$

Allo stesso modo, $p = ab$, $b > 1 \Rightarrow a < p \Rightarrow p \nmid a$

□

TEOREMA FONDAMENTALE DELL'ARITMETICA

Ogni numero naturale $n > 1$ è un numero primo o si può esprimere come prodotto di numeri primi.

Tale rappresentazione è unica, se si prescinde dall'ordine in cui comparemo i fattori.

DIM

DIM. DEL'ESISTENZA DI UNA FATTOORIZZAZIONE DI n :

$P(n) = \{n \text{ è un prodotto di numeri primi}\}$

$P(2)$ vera (2 è primo)

Supponiamo $P(2), \dots, P(n)$ vere

CASO 1: $n+1$ è primo

$P(n+1)$

CASO 2: $n+1$ è composto $\Rightarrow n+1 = ab$ con $1 < a, b < n+1$

ma $P(a), P(b)$ vere $\Rightarrow a = p_1^{u_1} \dots p_k^{u_k}$

con p_1, \dots, p_k primi

$\Rightarrow b = q_1^{v_1} \dots q_k^{v_k}$

con q_1, \dots, q_k primi

$\Rightarrow a$ e b sono primi o prodotto di primi

DIM. DELL'UNICITÀ DELLA FATTORIZZAZIONE:

Sia $S = \{n \in \mathbb{N}^*: n \text{ ha due fattORIZZAZIONI diverse}\}$

$S \neq \emptyset \Rightarrow n = \min(S)$

$n = p_1 \dots p_k$

$n = q_1 \dots q_l$ due diverse fatt. di n

$p_1 | n \Rightarrow p_1 | q_j$ per un qualche j (per il Lemmata di Euclide)

$\xrightarrow{\text{wg}} p_1 | q_i$ ma poiché p_1, q_i sono primi $\Rightarrow p_1 = q_i$

Allora m ha due fatt. distinte:

$m = p_2 \dots p_k$

$m = q_2 \dots q_l$

ma $m < n$, che contraddice la minimalità di n

$\Rightarrow S = \emptyset$, la fatt. di n è unica

□

PROPOSIZIONE (DEF mcm)

Siamo a e b interi diversi da zero.

Allora $|ab| = \text{mcm}(a, b) \cdot \text{MCD}(a, b)$

DIH

WLOG $a, b > 0$

Sia $S = \{ \text{fattori primi di } a \text{ e } b \} = \{ p_1, \dots, p_m \}$

Allora:

$$a = p_1^{a_1} \cdots p_m^{a_m}$$

$$b = p_1^{b_1} \cdots p_m^{b_m}$$

dove a_j, b_j possono anche essere nulli

$a_1, \dots, a_m = \text{fatt. primi di } a$

$b_1, \dots, b_m = \text{fatt. primi di } b$

$$\text{mcm}(a, b) = p_1^{\max(a_1, b_1)} \cdots p_m^{\max(a_m, b_m)}$$

$$\text{MCD}(a, b) = p_1^{\min(a_1, b_1)} \cdots p_m^{\min(a_m, b_m)}$$

$$\Rightarrow \text{mcm}(a, b) \cdot \text{MCD}(a, b) = p_1^{\max(a_1, b_1) + \min(a_1, b_1)} \cdots p_m^{\max(a_m, b_m) + \min(a_m, b_m)} = ab$$

$$\Rightarrow \text{mcm}(a, b) = \frac{ab}{\text{MCD}(a, b)}$$

□

Siamo a, b, c tre interi diversi da zero.

Allora:

$$\text{MCD}(a, b, c) = \text{MCD}(\text{MCD}(a, b), c)$$

$$\text{mcm}(a, b, c) = \text{mcm}(\text{mcm}(a, b), c)$$

In generale:

$$\text{MCD}(s_1, \dots, s_k) = \text{MCD}(\text{MCD}(s_1, \dots, s_{k-1}), s_k)$$

$$\text{mcm}(s_1, \dots, s_k) = \text{mcm}(\text{mcm}(s_1, \dots, s_{k-1}), s_k)$$

TEOREMA DEI NUMERI PRIMI

Sia $\pi: (1, \infty) \rightarrow \mathbb{N}^*$ la funzione

$\pi(x)$ = Numero di primi $\leq x$

Sia $\log x = \ln x$

Allora $\lim_{x \rightarrow \infty} \frac{\pi(x)}{\left(\frac{x}{\log x} \right) \eta(x)} = 1$

NOTA: Questo teorema indica che l'errore relativo

$$\frac{|\pi(x) - \eta(x)| \frac{x}{\log x}}{\left| \frac{x}{\log x} \right|} \rightarrow 0 \text{ per } x \rightarrow \infty$$

in quanto $\pi(x) \sim \frac{x}{\log x}$ cioè: il # di primi $\leq x$ tende a $\frac{x}{\log x}$ per $x \rightarrow \infty$

ma non fornisce alcuna informazione sull'errore assoluto $|\pi(x) - \eta(x)| \frac{x}{\log x}$

COROLARIO $p_n \sim n \log n$ dove $p_n = n\text{-esimo num. primo}$

(equivalente al th dei numeri primi)

DIM (commi)

$$\pi(p_n) = n \Rightarrow \pi^{-1}(n) = p_n \text{ dove } \pi(x) \sim \frac{x}{\log x}$$

□

IPOTESI DI DEDEKIND (IRRISOLTA)

$$|\pi(x) - \text{Li}(x)| < \sqrt{x} \log x, \quad x \geq 2.01$$

dove $\text{Li}(x) = \int_2^x \frac{dt}{\log t}$

TEOREMA (EULER)

La serie $\sum_{p:\text{primo}} \frac{1}{p}$ è divergente.

(cioè $\lim_{x \rightarrow \infty} \sum_{p:\text{primo}} \frac{1}{p} = \infty$)

PERCHÉ IN GENERALE

$$\sum_{j=1}^{\infty} a_j \rightarrow L \Rightarrow \left| \sum_{j=k}^{\infty} a_j \right| < \epsilon$$

DIM (Erdős)

Sia p_j il j -esimo numero primo.

Se la serie converge $\exists k$ intero più piccolo t.c. $\sum_{j=k+1}^{\infty} \frac{1}{p_j} < \frac{1}{2}$

$\forall l \in \mathbb{N}^*$ sia S_l il sottoinsieme di $\{1, \dots, l\}$ costituito da elementi che possono essere scritti come prodotti dei primi $\{p_1, \dots, p_k\}$.

LIMITE SUPERIORE PER LA CARDINALITÀ DI S_l :

Ogni elemento di S_l può essere scritto come un prodotto $a^2 b$ dove b è un intero privo di quadrati (cioè non è divisibile per nessun quadrato perfetto tranne 1).

Il numero di possibili scelte per b è quindi 2^k perché $b = p_1^{e_1} \dots p_k^{e_k}$ dove ogni $e_j \in \{0, 1\}$.

Il numero di possibili scelte per a è sup. delimitato da \sqrt{l} . Quindi $|S_l| \leq \sqrt{l} 2^k$

LIMITE INFERIORE PER LA CARDINALITÀ DI S_l :

Sia $S'_l = \{1, \dots, l\} - S_l$

Ogni elemento di S'_l ha un fattore primo $> p_k$.

Sia $S_l(j) = \{s \in S_l : p_j | s\}$

Si noti che $S_l(j) = \emptyset$ per $p_j > l$

Allora $S'_l = \bigcup_{j>k} S_l(j)$

Inoltre la cardinalità di $S_l(j)$ è al max. $\frac{l}{p_j}$

Allora $|S'_2| \leq \sum_{j=k+1}^{\infty} |S_2(j)| \leq \sum_{j=k+1}^{\infty} \frac{\varrho}{p_j} < \frac{\varrho}{2}$ per (*)

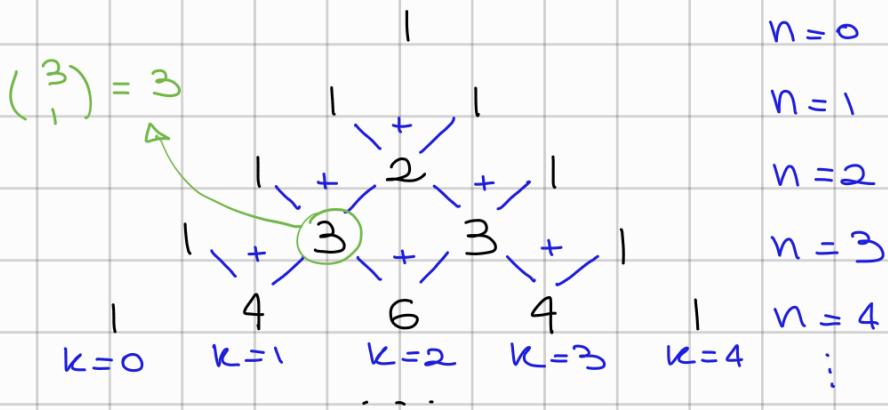
Ma $|S'_2| = \varrho - |S_2|$

Quindi $\varrho - |S_2| \leq \frac{\varrho}{2} \Rightarrow \frac{\varrho}{2} \leq |S_2|$

$\Rightarrow \frac{\varrho}{2} \leq |S_2| \leq \sqrt{\varrho} 2^k$ che è falso per $\varrho > 2^{2k+2}$

□

TRIANGOLIO DI PASCAL



Le cui voci sono i coefficienti binomiali:

$$\text{binomiale} \binom{n}{k} = \binom{n}{k} = \frac{n!}{k!(n-k)!}, \quad n \geq k$$

in particolare $\binom{n}{0} = 1 \quad \forall n \geq 0$

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

$$\binom{0}{k} = 0$$

REGOLA DI PASCAL

Siamo $n, k \in \mathbb{N}^*$

$$\text{Allora } \binom{n-1}{k} + \binom{n-1}{k-1} = \binom{n}{k}$$

DIM

$$\binom{n-1}{k} + \binom{n-1}{k-1} = \frac{(n-1)!}{k!(n-1-k)!} + \frac{(n-1)!}{(k-1)!(n-k)!} =$$

$\underbrace{}_{n-k-1}$

$$= (n-1)! \left[\frac{n-k}{k!(n-k)!} + \frac{k}{k!(n-k)!} \right] =$$

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

□

TEOREMA BINOMIALE

Sia n un intero non negativo.

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

DIM

Per induzione:

- $n=0: (x+y)^0 = 1 \quad \checkmark$

- $n+1: (x+y)^{n+1} = (x+y)^n (x+y) = \left(\sum_{k=0}^n \binom{n}{k} x^k y^{n-k} \right) (x+y) =$
 $= \sum_{k=0}^n \binom{n}{k} x^{k+1} y^{n-k} + \sum_{k=0}^n \binom{n}{k} x^k y^{n+1-k} =$
 $= x^{n+1} + \sum_{k=0}^{n-1} \binom{n}{k} x^{k+1} y^{n-k} + y^{n+1} + \sum_{k=1}^n \binom{n}{k} x^k y^{n+1-k} =$
 $= x^{n+1} + y^{n+1} + \sum_{k=1}^n \left[\binom{n}{k-1} + \binom{n}{k} \right] x^k y^{n+1-k}$
 $= x^{n+1} + y^{n+1} + \sum_{k=1}^n \underbrace{\binom{n+1}{k}}_{\text{RECURSE, PER LA REGOLA DI PASCAL}} x^k y^{n+1-k}$
 $= \sum_{k=0}^{n+1} \binom{n+1}{k} x^k y^{n+1-k}$
 $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$

$\Rightarrow \binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$

LEMMA

Sia p un numero primo e k un intero t.c. $0 < k < p$.

Allora p è un divisore di binomiale (p, k) .

DIM

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} \Rightarrow k!(p-k)!\binom{p}{k} = p!$$

$p | p!$ perché $p! = p(p-1)!$

Per il Lemma di Euclide $p | k! \circ p | (p-k)! \circ p | \binom{p}{k}$

Ma poiché $0 < k < p$, $p \nmid k!$, $p \nmid (p-k)!$

$$\Rightarrow p | \binom{p}{k}$$

□

PICCOLO TEOREMA DI FERMAT

Sia p un numero primo e n un intero.

Allora $p | n^p - n$

DIM

$$P(n): p | n^p - n$$

Supponiamo $P(n)$ vera per $n > 0$. Allora $P(n)$ vera per $n < 0$

$$\begin{aligned} p=2 \Rightarrow f(n) &= n^2 - n \Rightarrow f(-n) = n^2 + n = f(n) + 2n \\ \Rightarrow 2 | f(n) &\Rightarrow 2 | f(-n) \end{aligned}$$

$$p > 2 \Rightarrow f(n) = n^p - n \Rightarrow f(-n) = -n^p + n = -f(n)$$

$P(0)$ è vera - Supponiamo $P(n)$ vera -

Allora:

$$\begin{aligned} (n+1)^p - (n+1) &= \sum_{k=0}^p \binom{p}{k} n^k - (n+1) = \\ &= (n^p + 1) + \sum_{k=1}^{p-1} \binom{p}{k} - (n+1) = \\ &= (n^p - n) + \sum_{k=1}^{p-1} \binom{p}{k} \end{aligned}$$

Per ipotesi induttiva $p | n^p - n$

Per il lemma precedente p è un divisore di binomiale (p, k) .

Allora $p | (n+1)^p - (n+1) \Rightarrow P(n+1)$ è vera.

□

$\mathbb{Q}[x]$ = insieme dei polinomi nella variabile x con coefficienti razionali

$P_n[x]$ = sottospazio vettoriale di $\mathbb{Q}[x]$ che consiste di tutti gli elementi che possono essere scritti come:

$$f(x) = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \dots + \alpha_0, \quad \alpha_n, \dots, \alpha_0 \in \mathbb{Q}$$

$\deg(f) = n$ se $\alpha_n \neq 0$

$\deg(0)$ è indefinito

NOTA: con i num. razionali non è possibile matematizzare un vettore, trovare gli autovettori ecc.
(seconda parte corso algebra lineare)

DEF Siamo $f, g \in \mathbb{Q}[x]$.

Allora $f \mid g \Leftrightarrow \exists h \in \mathbb{Q}[x] \text{ t.c. } f \cdot h = g$

DEF (POLINOMIO MONICO)

$f \in \mathbb{Q}[x]$ è un polinomio monico \Leftrightarrow il coefficiente del termine di grado massimo è 1

Per definire $\text{mcm}(f, g)$ com $f, g \in \mathbb{Q}[x]$ non nulli:
 Sia: $S = \{h \in \mathbb{Q}[x] - \{0\} : f|h, g|h\}$
 Allora $S \neq \emptyset$ perché $f, g \in S$

DEF (mcm TRA DUE POLINOMI)

$\text{mcm}(f, g) = m \in S : m \text{ è monico e } \deg(m) \text{ è minimo}$

LEMMA S contiene un unico polinomio monico di grado min.

DIM

ESISTENZA

$$S = \{h \in \mathbb{Q}[x] - \{0\} : f|h, g|h\}$$

$\Rightarrow \exists$ il più piccolo intero positivo d t.c. $S \cap \mathbb{P}_d[x] \neq \emptyset$
 $h \in S \cap \mathbb{P}_d[x] \Rightarrow$ dopo avere riscalato h , h è monico

(*) PERCHÉ SE $f \in \mathbb{Q}[x] - \{0\}$, $f = a_n x^n + \dots + a_0$, $a_n \neq 0$

posso scrivere f così $\frac{1}{a_n} f = x^n + \dots + a_0$ E RENDERLO MONICO

NOTA: NON È POSSIBILE FARLO SE $f \in \mathbb{Z}[x] - \{0\}$

IN QUESTO CASO mcm POTREBBE NON ESISTERE

UNICITÀ

Supponiamo $h, h' \in S \cap \mathbb{P}_d[x]$ polinomi monici
 di grado d.

$$h = a_d x^d + \dots + a_0$$

$$h' = b_d x^d + \dots + b_0$$

$$a_d = b_d = 1$$

$$\Rightarrow \underbrace{h - h'}_{\downarrow} = 0 \text{ oppure } \deg(h - h') < d$$

$$h = h'$$

Supponiamo $h - h' \neq 0$. Allora:

$$f|h, f|h', g|h, g|h' \Rightarrow f|(h - h'), g|(h - h')$$

$\Rightarrow h - h' \in S$, $\deg(h - h') < h, h' \downarrow \uparrow$ perché il grado minimo è d

ESEMPIO

$$f_1 = x^3 - 1 = (x-1)(x^2 + x + 1)$$

$$f_2 = x^2 - 3x + 2 = (x-1)(x-2)$$

$$\text{mcm}(f_1, f_2) = (x-1)(x^2 + x + 1)(x-2)$$

$$\text{MCD}(f_1, f_2) = (x-1)$$

TEOREMA (ANALOGO DEL TH DI DIVISIONE PER I POLINOMI)

Siamo $f, g \in \mathbb{Q}[x]$, $\deg(g) > 0$.

Allora $\exists! q, r \in \mathbb{Q}[x]$ t.c. $f(x) = q(x)g(x) + r(x)$

dove $r(x) = 0$ oppure $\deg(r) < \deg(g)$

DIM (per induzione su $\deg(f)$)

Sia $d = \deg(g)$

Se $f=0$ oppure $\deg(f) < d$ poniamo $q=0, r=f$

Per $n \geq d$ sia $P(n) = \begin{cases} \deg(f) < n \Rightarrow \exists q, r \in \mathbb{Q}[x] \text{ t.c.} \\ f = qg + r \text{ dove } r=0 \text{ oppure } \deg(r) < \deg(g) \end{cases}$

$$\overset{n=d}{\uparrow}$$

Per verificare $P(d)$, siamo:

$$f = f_d x^d + \dots + f_0$$

$$g = g_d x^d + \dots + g_0$$

$$\text{Siamo } q = \frac{f_d}{g_d} \text{ e } r = f - qg$$

$$\overset{d}{\downarrow}$$

$\Rightarrow f = qg + r, r=0$ oppure $\deg(r) < \underbrace{\deg(g)}$ perché
abbiamo eliminato il termine di grado più alto di f

Supponiamo $P(d), \dots, P(n)$ vere

$$\text{Sia } f(x) = f_{n+1} x^{n+1} + \dots + f_0$$

$$\text{Poniamo } q_{n+1-d} = \left(\frac{f_{n+1}}{g_d} \right) x^{n+1-d} \text{ e } \tilde{f} = f - q_{n+1-d} g$$

Allora $\deg(\tilde{f}) < n+1$ perché abbiamo eliminato il termine di grado più alto di f .

Baie l'ipotesi induttiva $\exists q, r \in \mathbb{Q}[x]$ t.c. $\tilde{f} = qg + r$ dove $r = 0$ oppure $\deg(r) < \deg(g)$

$$\Rightarrow \tilde{f} = f - q_{n+1-d}g = qg + r \Rightarrow f = (q_{n+1-d} + q)g + r$$

$$\Rightarrow P(n+1) \text{ vera}$$

□

Perc definiere $\text{MCD}(f, g)$ com $f, g \in \mathbb{Q}[x]$ non nulli
sia: $T = \{af + bg \in \mathbb{Q}[x] - \{0\} : a, b \in \mathbb{Q}[x]\}$

Allora $T \neq \emptyset$ perché $f + g \in T$

DEF (MCD TRA DUE POLINOMI)

$\text{MCD}(f, g) = m \in T : m \text{ è monico e } \deg(m) \text{ è minimo}$

LEMMA T contiene un unico polinomio monico di grado min.

DIM

· ESISTENZA

$T \neq \emptyset$ perché $f + g \in T$

$\Rightarrow \exists$ il più piccolo intero positivo d t.c. $T \cap \mathbb{P}_d[x] \neq \emptyset$

$h \in T \cap \mathbb{P}_d[x] \Rightarrow$ dopo avere reiscalato h , h è monico

· UNICITÀ

Supponiamo $h, h' \in T \cap \mathbb{P}_d[x]$ polinomi monici
di grado d .

$$h = a_d x^d + \dots + a_0$$

$$h' = b_d x^d + \dots + b_0$$

$$a_d = b_d = 1$$

$$\Rightarrow \underline{h - h' = 0} \text{ oppure } \deg(h - h') < d$$

$$\Rightarrow h = h'$$

Supponiamo $h - h' \neq 0$. Allora:

$h = af + bg$, $\tilde{h} = \tilde{a}f + \tilde{b}g \Rightarrow h - h' = (\tilde{a} - a)f + (\tilde{b} - b)g \in T \cap P_{\mathbb{Q}}[x]$
che contraddice la minimialità dei gradi di h e h' .

□

LEMMA

Siano $f, g \in \mathbb{Q}[x]$ t.c. $(f, g) \neq (0, 0)$.

Sia h l'unico polinomio monico di T di grado minimo.

Allora $h|f$ e $h|g$.

DIM

$$f = 0 \Rightarrow h = cg, c \neq 0$$

cioè h è l'unico polinomio monico multiplo scalare di g

$$g = 0 \Rightarrow h = cf, c \neq 0$$

Rimane da considerare il caso $f \neq 0, g \neq 0$:

$$f, g \in T \Rightarrow \deg h \leq \min(\deg(f), \deg(g))$$

Siamo:

$$h = af + bg$$

$$f = qh + r \text{ dove } r=0 \text{ oppure } \deg(r) < \deg(h)$$

Se $r=0 \Rightarrow h|f$, altrimenti:

$$f = q(af + bg) + r \Rightarrow r = (1-q)a f - qb g \in T$$

→ CONTIENE TUTTE LE
COMB. LINEARI A
COEFF. RAZIONALI DI f E g

Per la minimialità del grado di h , dobbiamo avere $r=0$ ($\Rightarrow h|f$).

Lo stesso vale per g .

□

Per analogia con gli interi:

$$f = qg + r \Rightarrow \text{MCD}(f, g) = \text{MCD}(qg + r, g) = \text{MCD}(r, g) = \text{MCD}(g, r)$$

Un polinomio costante è un polinomio della forma

$f(x) = f_0$ per qualche $f_0 \in \mathbb{Q}$.

In particolare, un polinomio non costante ha grado maggiore di zero.

DEF (POLINOMIO IRREDUCIBILE)

Un polinomio $f \in \mathbb{Q}[x]$ non costante è irriducibile se non esistono polinomi non costanti $g, h \in \mathbb{Q}[x]$ t.c. $f = gh$. Altrimenti è riducibile.

ESEMPI

i) Un polinomio di grado 1 è irriducibile.

DIM

$$f = gh \text{ con } g, h \text{ pol. non costanti} \Rightarrow \deg(g), \deg(h) \geq 1$$
$$\Rightarrow \deg(f) = \deg(g) + \deg(h) > 1 \quad \frac{\downarrow}{\uparrow}$$

ii) f irriducibile e $c \in \mathbb{Q} - \{0\} \Rightarrow cf$ irriducibile

iii) se $f \in \mathbb{Q} - \{0\}$ ha una radice razionale $x = r$

$\Rightarrow f$ è riducibile perché $(x - r) | f$

DIM

$$f = f_n x^n + \dots + f_0 = f_n (x - r)^n + \tilde{f}_n (x - r)^{n-1} + \dots + \tilde{f}_0$$

$$\begin{aligned} &\{x^n, \dots, 1\} \\ &\{(x - r)^n, (x - r)^{n-1}, \dots, 1\} \end{aligned} \quad \begin{matrix} \nearrow \\ \searrow \end{matrix} \quad \text{BASI DI } \mathbb{P}_n[x]$$

$$f(r) = \tilde{f}_0 \Rightarrow f(r) = 0 \Rightarrow x - r | f$$

iv) Sia $f \in \mathbb{Q}[x]$ un polinomio di grado 2.

Allora f è irriducibile $\Leftrightarrow f$ non ha una radice razionale.

DIM

$$P = \{f \text{ è irriducibile}\}$$

$$Q = \{f \text{ non ha una radice razionale}\}$$

Il contracompromissore di $P \Rightarrow Q$ è $\neg Q \Rightarrow \neg P$, ovvero: se f ha una radice razionale allora f è riducibile.

Il controaccordatore di $Q \Rightarrow P$ è $\neg P \Rightarrow \neg Q$, ovvero: se f è riducibile allora f ha una radice razionale.

Poiché $\deg(f) = 2$, f riducibile $\Rightarrow f = gh$ dove $\deg(g), \deg(h) = 1 \Rightarrow \deg(f) > 1$
 $\Rightarrow f$ ha una radice razionale.

LEMMA

Siamo $f, g \in \mathbb{Q}[x]$.

f irriducibile $\Rightarrow \text{MCD}(f, g) = 1$ oppure $f \mid g$

DIM

Sia $m = \text{MCD}(f, g)$.

Allora $m \mid f \Rightarrow f = mq$ per un qualche $q \in \mathbb{Q}[x] - \{0\}$

Per def., poiché f è irriducibile, segue che o m o q ha grado 0, cioè $m = 1$ oppure $m = uf$ per un qualche $u \in \mathbb{Q}[x] - \{0\}$.

$m = 1 \Rightarrow m = \text{MCD}(f, g) = 1$

$m = uf \Rightarrow m = \text{MCD}(f, g) = uf \mid g \Rightarrow f \mid g$

LEMMA (ANALOGO DEL LEMMA DI EUCLIDE PER I POLINOMI)

Sia $f \in \mathbb{Q}[x]$ irriducibile -

Se $f \mid gh \Rightarrow f \mid g$ oppure $f \mid h$

DIM

In base al lemma precedente, $f \mid g \Rightarrow \text{gcd}(f, g) = 1$ oppure $f \mid g$ -

Dunque $\exists a, b \in \mathbb{Q}[x] + c.$ $af + bg = 1 \Rightarrow afh + bgh = h$
 $\Rightarrow f \mid afh, f \mid bgh \Rightarrow f \mid h$

TH DI FATTOORIZZAZIONE UNICA

Ogni polinomio non costante $f \in \mathbb{Q}[x]$ puo' essere scritto come prodotto di polinomi irriducibili -

Inoltre questa fattorizzazione e unica -

Se $f(x) = p_1(x) \cdots p_r(x)$ e $f(x) = q_1(x) \cdots q_s(x)$ sono due fattorizzazioni scritte come prodotto di polinomi irriducibili allora:

i) $r=s$

ii) Esiste una permutazione σ di $\{1, \dots, r\}$ e una collezione di costanti non nulle $\{c_j\} + c.$:

$$q_j(x) = c_j p_{\sigma(j)}(x) \quad \text{per } j=1, \dots, r$$

(cioe la fattorizzazione e unica a meno di moltiplicare per delle costanti:

$$\text{es.: } x^3 - x = x(x^2 - 1) = x(x+1)(x-1) = \left(\frac{1}{2}(x+1)\right)\left(\frac{1}{3}(x-1)\right)(6x)$$

DIM

1) Dimostriamo che ogni polinomio non costante $f \in \mathbb{Q}[x]$ è un prodotto di polinomi irriducibili

Usiamo l'induzione su $\deg(f)$

$P(n) = \{$ ogni polinomio di grado n può essere scritto come prodotto di fattori irriducibili $\}$

• $P(1)$, cioè $\deg(f) = 1$: (abbiamo escluso il caso di polinomio costante $\deg(f) = 0$)

$$f(x) = ax + b = gh \Rightarrow \deg(gh) = \deg(g) + \deg(h) \quad \checkmark$$

Supponiamo $P(1), \dots, P(n)$ vere.

• $P(n+1)$, cioè $\deg(f) = n+1$:

CASO 1: f è irriducibile

CASO 2: $f = gh$ dove $\deg(g), \deg(h) < \deg(f) = n+1$

per l'ipotesi induttiva g e h possono essere scritti come prodotto di pol. irriduc.

2) Dimostriamo l'unicità della fattorizzazione

Supponiamo di avere due fatt. di f :

$$(*) \quad f = p_1 \cdots p_r, \quad f = q_1 \cdots q_s$$

$p_i | f \Rightarrow p_i | q_j$ per qualche j (PER IL LEMMA DI EUCLIDE)
(VEDI ANCHE DIN TH. F. ARITM. LEZ 3)

p_j, q_j irriducibili $\Rightarrow q_j = c \cdot p_j$ per qualche $c \in \mathbb{Q} - \{0\}$

Dopo avere riordinato i fattori possiamo assum. $j=1$

Usiamo l'induzione sul numero totale di fattori $r+s$

$P(n) = \{$ se un polinomio non costante f ha una coppia di fattorizz. irriducibili t.c. $r+s \leq n$, allora $r=s$ e la fattorizz. è unica fino al riordino dei fattori e alla loro moltiplic. per elementi non nulli di \mathbb{Q} }

- $P(1)$ ✓ poiché im (*) ogni lato contiene almeno un fattore, un polinomio di questo tipo (quindi con $r+s \leq 1$) non può esistere
- $P(2)$ ✓ perché, in questo caso, $r=s=1$ e la fattorizz. è $f = p_1 = q_1$, dove $q_1 = c.p.$

Supponiamo $P(1), \dots, P(n)$ vere -

La fattorizz. assume la forma $p_1 p_2 \dots p_r = (c.p.) q_2 \dots q_s$
Dividendo entrambi i lati per p_1 e considerando c , parte di q_2 otteniamo $f = p_2 \dots p_r = q_2 \dots q_s$
dove il num. totale di fattori è:

$$(r-1) + (s-1) = \underbrace{r+s-2}_{n+1} = n+1-2 = n-1$$

Poiché $P(n-1)$ è vera, ne segue che:

i) $r-1 = s-1$

ii) la fattorizz. di f in fattori irriducibili è unica fino al riordino e alla moltiplic. per elementi non nulli di \mathbb{Q} .

□

COROLARIO

Siamo $f, g \in \mathbb{Q}[x]$ polinomi monici non costanti.

Allora $fg = \text{mcm}(f, g) \text{MCD}(f, g)$

DIM

Sia $\{p_1, \dots, p_n\}$ l'insieme dei fattori irrid. di f e g .

$$\Rightarrow f = p_1^{a_1} \cdots p_n^{a_n}, \quad g = p_1^{b_1} \cdots p_n^{b_n}$$

dove si assumono rispettivamente $a_j = 0$ o $b_j = 0$ se p_j non è un fattore di f o di g

Allora:

$$\begin{aligned} \text{mcm}(f, g) &= p_1^{\max(a_1, b_1)} \cdots p_n^{\max(b_1, b_n)} \\ \text{MCD}(f, g) &= p_1^{\min(a_1, b_1)} \cdots p_n^{\min(a_n, b_n)} \end{aligned}$$

$$\begin{aligned} \Rightarrow \text{mcm}(f, g) \text{MCD}(f, g) &= p_1^{\max(a_1, b_1) + \min(a_1, b_1)} \cdots p_n^{\max(a_n, b_n) + \min(a_n, b_n)} \\ &= p_1^{a_1+b_1} \cdots p_n^{a_n+b_n} = fg \end{aligned}$$

□

ESEMPIO

$$f = x^2 - 3x + 2 = (x-1)(x+2)$$

$$g = x^2 - 2x + 1 = (x-1)^2$$

$$\Rightarrow \text{MCD}(f, g) = (x-1)$$

$$\begin{aligned} \Rightarrow \text{mcm}(f, g) &= \frac{fg}{\text{MCD}(f, g)} = \frac{(x-1)(x+2)(x-1)^2}{(x-1)} = (x-1)^2(x+2) \\ &= x^3 - 4x^2 + 5x - 2 \end{aligned}$$

TEOREMA DELLE RADICI RAZIONALI

Sia $\mathbb{Z}[x] \subset \mathbb{Q}[x]$ l'insieme dei polinomi con coeff. interi.

Le radici razionali di un polinomio non costante $f \in \mathbb{Q}[x]$ t.c. $f(0) \neq 0$ possono essere trovate come segue:

Sia m il più piccolo intero positivo t.c. $g = mf \in \mathbb{Z}[x]$

Allora $f(r) = 0 \iff g(r) = 0$

Sia $g(x) = g_n x^n + \dots + g_0$ dove $g_n, g_0 \neq 0$

Allora ogni radice razionale di f è della forma $r = p/q$ dove $p|g_0, q|g_n, \text{MCD}(p, q) = 1$

[NOTA: non funziona per radici non razionali]

DIM

Si supponga $g(p/q) = 0$ con $\text{MCD}(p, q) = 1$

Allora $g(p/q) = g_n(p/q)^n + g_{n-1}(p/q)^{n-1} + \dots + g_0 = 0$

Moltiplicando entrambi i membri per q^n ottieniamo:

$$g_n p^n + g_{n-1} p^{n-1} q + \dots + g_0 q^n = 0$$

$$\Rightarrow p(g_n p^{-1} + \dots + g_1 q^{n-1}) = -g_0 q^n \Rightarrow p | g_0 q^n$$

Per ipotesi $\text{MCD}(p, q) = 1$, dunque $p | g_0$

$$\Rightarrow q(g_{n-1} p^{n-1} + \dots + g_0 q^{n-1}) = -g_n p^n \Rightarrow q | g_n p^n$$

Per ipotesi $\text{MCD}(p, q) = 1 \Rightarrow q | g_n$

□

ESEMPIO

$$f(x) = x^3 - 7x + 6$$

$$f(r) = 0, \quad r = \frac{p}{q}, \quad \text{MCD}(p, q) = 1$$

$$\left(\frac{p}{q}\right)^3 - 7\left(\frac{p}{q}\right) + 6 = 0$$

$$p^3 - 7pq^2 + 6q^3 = 0$$

$$p(p^2 - 7q^2) = -6q^3 \Rightarrow p \mid 6$$

$$q(-7pq + 6q^2) = -p^3 \Rightarrow q \mid 1$$

$$q = \pm 1$$

$$p = \{ \pm 1, \pm 2, \pm 3, \pm 6 \}$$

$$f(1) = 0$$

$$f(2) = 0$$

$$f(-3) = 0$$

$$\} \Rightarrow f = (x-1)(x-2)(x+3)$$

PROPOSIZIONE

Sia $f \in \mathbb{Z}[x]$ un polinomio non costante monico.

Allora ogni radice razionale di f è un numero intero.

DIM

$$f = x^n + f_{n-1}x^{n-1} + \dots + f_0$$

Sia $r \in \mathbb{Q}$ t.c. $r = \frac{p}{q}$, $f(r) = 0$, $\text{MCD}(p, q) = 1$

$$\Rightarrow p \mid f_0, q \mid 1 \Rightarrow r \in \mathbb{Z}$$

□

(+ vedi p. 6 LEZIONE 4 ultima parte per il metodo
rapido per trovare le radici razionali)

[PER CLASSI P, NP, NP-HARD VEDI VERSIONE 5 P.S.]

TEORIA DEI RETICOLI

DEF (RETCOLO)

Sia $B = \{b_1, \dots, b_m\}$ un insieme di vettori linearmente indipendenti in \mathbb{R}^n ($\Rightarrow m \leq n$).

Sia L lo spazio costituito dalle combinazioni lineari dei vettori contenuti in B : $L = \{\lambda_1 b_1 + \dots + \lambda_m b_m : \lambda_1, \dots, \lambda_m \in \mathbb{Z}\}$.

Allora L è un reticolo (tipo un sottospazio, ma a soli coeff. interi) e B è una base per L .

Per semplicità assumiamo $m=n$.

NOTA: la base B non è unica

ESEMPIO

$$L = \mathbb{Z}^n, B = \{e_1, \dots, e_n\}$$

ESEMPIO

Sia $n \geq 2$

$L = \{(x_1, \dots, x_n) \in \mathbb{Z}^n : 2 | (x_1 + \dots + x_n)\}$ è un reticolo con base:

$$\begin{cases} b_j = e_j - e_{j+1} & j=1, \dots, n-1 \\ b_n = e_n + e_{n-1} \end{cases}$$

perché:

$$2 | (x_1 + \dots + x_n) \Rightarrow x_1 + \dots + x_n = 2k$$

$$\Rightarrow \underbrace{(x_1 + \dots + x_n)}_{2k} - k(\underbrace{e_n + e_{n-1}}_2) \in \{y_1 + \dots + y_n = 0 \text{ b} \subseteq \mathbb{R}^n\}$$

\Rightarrow I VETTORI DI B SONO LIN. INDEPENDENTI

Un'altra base per L potrebbe essere:

$$B'_1: \{e_1 + e_2, e_2 - e_3, \dots, e_{n-1} - e_n\}$$

$$L(B) = L(B')$$

DEF (NORMA)

Per un numero reale $p \geq 1$, la p -norma di $x \in \mathbb{R}^n$ è definita da $\|(x_1, \dots, x_n)\|_p = (\|x_1\|^p + \dots + \|x_n\|^p)^{1/p}$.

Definiamo anche $\|(x_1, \dots, x_n)\|_\infty = \max(|x_1|, \dots, |x_n|)$

PROPOSIZIONE (PROPRIETÀ NORME)

$\forall p \geq 1$ la p -norma ha le seguenti proprietà:

- $\|x\|_p = 0 \iff x = 0$
- $\|\lambda x\|_p = |\lambda| \cdot \|x\|_p$
- $\|x+y\|_p \leq \|x\|_p + \|y\|_p$

TH (EQUIVALENZA TRA NORME)

Le norme $\|\cdot\|_p$ e $\|\cdot\|_q$ sono equivalenti se

$$\exists C, D \in \mathbb{R} \text{ t.c. } C\|x\|_p \leq \|x\|_q \leq D\|x\|_p \quad \forall x \in \mathbb{R}^n$$

DEF (SHORTEST VECTOR PROBLEM (SVP))

Il problema del vettore più breve nella norma p è il seguente:

- INPUT: una base B per un rettangolo L ;
- OUTPUT: il vettore non nullo più breve in B utilizzando la norma $\|\cdot\|_p$

TH (P. VAN ENDE BOAS, 1979)

SVP _{∞} è NP-HARD

Identifichiamo la base di un reticolo L con una matrice B $n \times n$ t.c. $B(\mathbb{Z}^n) = L$.

Sia T una mat. $n \times n$ con $\text{rk}(T) = n$ e valori interi.
Allora BT è la base per un nuovo reticolo.

NOTA: La base di L è costituita dalle colonne di B

$TB \Rightarrow$ si sta operando sullo spazio delle righe di B , ovvero la combinazione lineare delle righe

$BT \Rightarrow$ si sta operando sullo spazio delle colonne di B , ovvero la combinazione lineare delle colonne

ESEMPIO

$$B = (\vec{b}_1, \vec{b}_2), T = \begin{pmatrix} 1 & 0 \\ 2 & 3 \end{pmatrix}, BT = (\vec{b}_1 + 2\vec{b}_2, 3\vec{b}_2)$$

Per diminuire la dipendenza dalla scelta della base B di L , ricordiamo il seguente th:

TH

Sia T una matrice $n \times n$ con soli valori interi.

Allora T^{-1} esiste e ha solo valori interi $\Leftrightarrow \det(T) = \pm 1$

In questo caso si dice che T è una **mat. UNIMODULARE**

LEMMA

Sia T una matrice $n \times n$ invertibile con valori interi e B una base di un reticolo $L = L(B)$.

Allora $L(BT) \subseteq L(B)$

$$\text{DIN } \underbrace{\subseteq \mathbb{Z}^n}_{L(BT) = B \cdot (T(\mathbb{Z}^n))} \underbrace{= \lambda_1 \vec{b}_1 + \dots + \lambda_n \vec{b}_n}_{B(\mathbb{Z}^n) = L(B)}$$

dove $B = (\vec{b}_1, \dots, \vec{b}_n)$

sono vett. colonna

□

ESEMPIO

$$T = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$L(B) = \mathbb{Z}^2 \quad \xrightarrow{\text{PERCHÉ } T \text{ MOLTIPLICA PER 2}}$$

$$L(B^T) = B \underbrace{\left(2\mathbb{Z}^2 \right)}_{!!}$$

$$\left\{ \begin{pmatrix} 2a \\ 2b \end{pmatrix} : a, b \in \mathbb{Z} \right\}$$

TH

$$L(B) = L(C) \iff \exists U \text{ matrice unimodulare t.c. } C = BU$$

DIM

Per il lemma precedente, $C = BU \Rightarrow L(C) \subseteq L(B)$

Alllo stesso modo, $C = BU$ con U unimodulare $\Rightarrow B = CU^{-1}$

$$\Rightarrow L(B) = L(CU^{-1}) \subseteq L(C) \Rightarrow L(B) = L(C)$$

Viceversa, se $L(B) = L(C)$ allora $B = CT$ per qualche matrice T con valori interi (ogni $b \in B$ deve essere una combinazione lineare intera di elementi di C)

Poiché B e C sono entrambi una base di \mathbb{R}^n ,
 T è invertibile.

□

VOLUME DEL PARALLELEPIPEDO FONDAMENTALE

DATA UNA BASE $B = \{b_1, \dots, b_n\}$ DI L , IL PARALLELEPIPEDO FONDAMENTALE È:

$$P(B) = \{b_1x_1 + \dots + b_nx_n : x_1, \dots, x_n \in [0, 1]\}$$

IL VOLUME DI $P(B)$ È $|\det(B)|$.

Se C È UN'ALTRA BASE DI L , ALLORA $C = BU$ DOVE U È UNIMODULARE, QUINDI:

$$\text{vol}(P(C)) = |\det(C)| = |\det(BU)| = |\det(B) \cdot \det(U)| = |\det(B)| = \text{vol}(P(B))$$

DEF $\text{vol}(L) = |\det(B)|$ dove B è una qualsiasi base di L

In particolare, due basi che producono parallelepipedi fondamentali con volumi diversi definiscono reticolati diversi.

ESEMPIO

$B = \{(1, -1), (1, 1)\}$ e $C = \{(2, 3), (1, 2)\}$ definiscono reticolati diversi perché

$$|\det\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}| \neq |\det\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}|$$

NOTA: in \mathbb{R}^n si chiamano vett.-colonna

ESEMPIO

$B = \{(1, -1), (1, 1)\}$ e $C = \{(1, 0), (1, 2)\}$ definiscono reticolati diversi perché la somma delle coordinate dei vettori in B è sempre pari ($1-1=0, 1+1=2$) dunque ogni vettore in $L(B)$ ha questa proprietà.

Al contrario, la somma delle coordinate dei vettori in C è sempre dispari ($1+0=1, 1+2=3$) -

(nonostante $|\det(B)| = |\det(C)|$)

TH (BLICKFIELD)

Sia $L \subset \mathbb{R}^n$ un reticolo e $S \subseteq \mathbb{R}^n$ un insieme connesso t.c. $\text{vol}(S) > \text{vol}(L)$.

Allora esistono punti distinti $p_1, p_2 \in S$ t.c. $p_1 - p_2 \in L$.

(NOTA: ciò non implica $p_1, p_2 \in L$)

TH (MINKOWSKI)

Se $L \subseteq \mathbb{R}^n$ è un reticolato e S è un insieme di volume maggiore di $2^n \text{vol}(L)$ che è convesso e simmetrico rispetto all'origine.

Allora S contiene un punto non nullo di L .

DIM

Sia $S' = \frac{1}{2}S$ (cioè tutti gli elem. di S' sono uguali agli elem. di S divisi per 2)

Allora $\text{vol}(S') = 2^{-n} \text{vol}(S)$ e quindi $\text{vol}(S') > \text{vol}(L)$

Per il th di Blichfield, $\exists p_1, p_2$ distinti $\in S'$ t.c. $p_1 - p_2 \in L$

Poiché $S' = \frac{1}{2}S$ si ha $2p_1, 2p_2 \in S$

$\Rightarrow -2p_1, -2p_2 \in S$ perché S è simm. rispetto all'origine

$\Rightarrow \underbrace{p_1 - p_2}_{\in L} = \frac{1}{2}(2p_1 + (-2p_2)) \in S$ perché S è convesso quindi
 $2p_1, -2p_2 \in S \Rightarrow \frac{2p_1 - 2p_2}{2} \in S$

□

Il volume $V_n(r)$ della palla

$$B_n(r) = \{x = (x_1, \dots, x_n) \in \mathbb{R}^n : \|x\| \leq r\}$$

di raggio r im \mathbb{R}^n è dato dalla formula:

PER n PARI:

$$\underline{V_{2n}(r)} = \frac{\pi^n}{n} r^{2n}$$

IN DIMENSIONE $2n$

PER n DISPARI:

$$V_{2n+1}(r) = \frac{2(\kappa)(4\pi)^n}{(2k+1)} r^{2n+1}$$

Per semplificare la formula successiva scriviamo

$$V_n(r) = \gamma_n r^n$$

COROLARIO

Dato un reticolato $L \subseteq \mathbb{R}^n$, sia $\lambda_1(L)$ la lunghezza del vettore non nullo più corto im L rispetto alla norma euclidea. Allora:

$$\lambda_1(L) \leq 2 \left(\frac{\text{vol}(L)}{\gamma_n} \right)^{1/n}$$

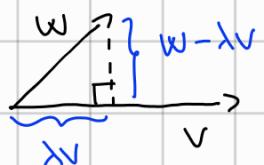
DIM

$$r > 2 \left(\frac{\text{vol}(L)}{\gamma_n} \right)^{1/n} \Rightarrow V_n(r) = \gamma_n r^n > \gamma_n 2^n \left(\frac{\text{vol}(L)}{\gamma_n} \right) = 2^n \text{vol}(L)$$

Portanto, per il Th di Minkowski, ogni palla di questo tipo contiene un vettore reticolare non nullo e quindi il vettore più breve di L diverso da zero.

ALGORITMO DI GAUSS

SVP è difficile per $n >> 0$, per $n=2$ si usa l'algoritmo di Gauss.



$$\begin{aligned} 0 &= (w - \lambda v, v) = (w, v) - \lambda(v, v) \Rightarrow \lambda = \frac{(w, v)}{(v, v)} \\ \lambda v &= \frac{(w, v)}{(v, v)} v \end{aligned}$$

IN GENERE $\lambda \in \mathbb{Z}$
 $\Rightarrow \lambda$ RETICOLO L

L'algor. di Gauss arretonda all'intero più vicino (se si ha $x.5$ arretonda all'intero pari più vicino).

L'algor. restituisce un vettore non nullo più corto generato da $B = \{v_1, v_2\}$ con complessità $O(\log(|v_1| + |v_2|))$

Sia $L = L(B) \subseteq \mathbb{R}^2$, dove $B = \{v_1, v_2\}$

DUNQUE LA
PROIEZ. DI
 v_1 SU v_2 R
NON È
PERPENDIC.

APROSS. PERCHE'
SI ARRETONDA
ALL'INTERO R
PIÙ VICINO

- Se $|v_2| < |v_1|$ scambiare v_1 e v_2 ;
- Sia $v_2^* = v_2 - m v_1$, dove $m = \left\lfloor \frac{(v_1, v_2)}{|v_1|^2} \right\rfloor$;

PASSAGGIO
CHIAVE:
→ FORMA APROSS.
DI PROIEZ.
ORTOGONALE

- se $m = 0$ restituire la base $\{v_1, v_2\}$;
- in caso contrario, sostituire v_2 con v_2^* e ripetere i passaggi precedenti

AD OGNI PASSO SI
RIDUCE LA LUNG.
DEI VET. BASE

LEMMA

Sia $\{v_1, v_2\}$ il risultato dell'algoritmo di Gauss.
Allora v_1 è un vettore più breve di L .

DIM

Al termine dell'algoritmo sappiamo che (condizioni di terminazione):

- i) $|v_1| \leq |v_2|$ PERCHÉ SE $|v_2| < |v_1|$ $v_1 \in v_2$ SI SCAMBIANO
- ii) $\frac{|(v_1, v_2)|}{|v_1|^2} \leq \frac{1}{2}$ PER L.T.

Sia $v = c_1 v_1 + c_2 v_2 \in L$.

Allora:

$$\begin{aligned}
 |v|^2 &= (c_1 v_1 + c_2 v_2, c_1 v_1 + c_2 v_2) = \\
 &= c_1^2 |v_1|^2 + 2c_1 c_2 (v_1, v_2) + c_2^2 |v_2|^2 \\
 &\stackrel{(*)}{\geq} c_1^2 |v_1|^2 - 2|c_1 c_2| |(v_1, v_2)| + c_2^2 |v_2|^2 \\
 &\geq c_1^2 |v_1|^2 - |c_1 c_2| |v_1|^2 + c_2^2 |v_2|^2 \quad \left. \right\} \text{ PER i) E ii)} \\
 &\geq (c_1^2 - |c_1 c_2| + c_2^2) |v_1|^2
 \end{aligned}$$

(*) NON CONOSCIAMO I
SEGNI DI c_1, c_2 E
 (v_1, v_2) QUINDI
RETTIFIAMO IL VAL-
ASSOLUTO E ROI IL
"—" PER GIUSTIFICARE
LA DISEGUAGLIANZA

$$\text{dove } c_1^2 - |c_1 c_2| + c_2^2 = \underbrace{(|c_1| - |c_2|)^2}_{\geq 0} + |c_1 c_2| \geq 0 \in \mathbb{Z}$$

Dunque è sufficiente dim. che:

$$(c_1, c_2) \neq (0, 0) \Rightarrow c_1^2 - |c_1 c_2| + c_2^2 > 0$$

Poiché $c_1^2 - |c_1 c_2| + c_2^2$ non cambia al variare dei segni di c_1 e c_2 possiamo assumere $c_1, c_2 \geq 0$ e verificare che:

$$\begin{aligned}
 c_1^2 - c_1 c_2 + c_2^2 &\geq 0 \\
 \Rightarrow \underline{(c_1 - c_2)^2 + c_1^2 + c_2^2} \geq 0 \quad \forall (c_1, c_2) \neq (0, 0)
 \end{aligned}$$

ESEMPIO

$$u = (2, 3) = v_1$$

$$v = (5, 8) = v_2$$

$|v_2| > |v_1| \Rightarrow$ non serve scambiare v_1 e v_2

$$v_2^* = v_2 - \left[\frac{(v_1, v_2)}{|v_1|^2} \right] v_1 = (5, 8) - \left[\frac{3}{13} \right] (2, 3) = (-1, -1)$$

$$\{(2, 3), (-1, -1)\}$$

$$|v_2| < |v_1| \Rightarrow \{(-1, -1), (2, 3)\}$$

$$v_2^* = (2, 3) - 2(-1, -1) = (0, 1)$$

$$\{(-1, -1), (0, 1)\}$$

$$|v_2| < |v_1| \Rightarrow \{(0, 1), (-1, -1)\}$$

$$v_2^* = (-1, -1) - (-1)(0, 1) = (-1, -1) - (0, -1) = (-1, 0)$$

$$\{(0, 1), (-1, 0)\}$$

$$|v_1| \leq |v_2|, \left[\frac{(v_1, v_2)}{|v_1|^2} \right] = 0 \Rightarrow (0, 1) \text{ è un vettore di lunghezza minima in } L$$

Per costruire questi sistemi utilizzando i reticolati sono essenziali:

- una base di vettori brevi per il reticolo (K_{priv})
- una base di vettori lunghi per il reticolo (K_{pub})

[ES. CIFRARIO "NTQU" (CRITTOGRAFIA BASATA SUI RETICOLI) IL CUI PROCESSO DI CIFRATURA SI BASA SU SVP]

Per questo motivo vorremmo essere in grado di costruire matrici unimodulari con voci molto grandi. Consideriamo la matrice

$$M = \begin{pmatrix} x & y \\ ny & x \end{pmatrix} \Rightarrow \det(M) = x^2 - ny^2, n \in \mathbb{Z}$$

Allora M è unimodulare $\Leftrightarrow x, y \in \mathbb{Z}$ e $\det(M) = \pm 1$
avendo se $x^2 - ny^2 = 1$ EQUAZIONE DI PELL

L'equazione di Pell ha un numero infinito di soluzioni $(1,0), (x_1, y_1), (x_2, y_2), \dots$ che possono essere trovate utilizzando la relazione di ricorrenza (Brahmagupta):

$$x_{k+1} = x_k x_k + ny_k y_k, \quad y_{k+1} = x_k y_k + y_k x_k$$

All'origine della relazione di ricorrenza vi è il seguente lemma:

LEMMA Se A e B sono matrici $n \times n$ unimodulari, anche AB è unimodulare. Se A è unimodulare lo è anche A^T .

DIM $\underbrace{\pm 1}_{\det(A)} \quad \underbrace{\pm 1}_{\det(B)}$

$$\det(AB) = \det(A)\det(B) = \pm 1 \Rightarrow AB \text{ unimodulare}$$

$$\det(A) = \det(A^T) = \pm 1 \Rightarrow A^T \text{ unimodulare}$$

□

In particolare, siamo:

$$A = \begin{pmatrix} x & y \\ ny & x \end{pmatrix}, \quad B = \begin{pmatrix} u & v \\ nv & u \end{pmatrix} \text{ dove } \det(A) = x^2 - ny^2 = 1, \det(B) = u^2 - nv^2 = 1$$

Allora:

$$AB = \begin{pmatrix} xu + ynv & xv + yu \\ nyu + xnv & nyv + xu \end{pmatrix} = \begin{pmatrix} r & s \\ ns & r \end{pmatrix}$$

$$\det(AB) = \underbrace{\det(A)}_{=1} \underbrace{\det(B)}_{=1} = r^2 - ns^2$$

$$\text{In generale } A = \begin{pmatrix} x_1 & y_1 \\ ny_1 & x_1 \end{pmatrix} \Rightarrow A^k = \begin{pmatrix} x_k & y_k \\ ny_k & x_k \end{pmatrix}$$

TH Ogni matrice intera 2×2 con determinante 1 può essere scritta come prodotto finito delle matrici

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Il prodotto vuoto è la matrice identità

NOTA: la moltiplicazione tra matrici non è commutativa dunque la rapp. di una mat. come prodotto di S e T non è unica

L'utilizzo dell'equazione di Pell in questo modo presenta almeno 3 problemi:

1) le soluzioni dell'eq. di Pell presentano una struttura che potrebbe facilitare la violazione del sistema critografico

- 2) non è solo un algoritmo che trovi le soluzioni
dell' eq. di Bell in tempo polinomiale
3) funziona solo per matrici 2×2

Possiamo superare i problemi 1 e 2 tramite il
seguente algoritmo probabilistico.

PROBLEMA: Generare casualmente matrici 2×2 con voci
interi e $\det(A) = \pm 1$

SOLUZIONE: Generare casualmente due numeri interi
grandi A e B.

La probab. che $\text{MCD}(A, B) = 1$ è $6/\pi^2$ perché:

$$\sum \frac{1}{n^2} = \frac{\pi^2}{6} = \prod_{p: \text{primo}} \frac{1}{1-p^{-2}}$$

$$\Rightarrow \prod_{p: \text{primo}} (1-p^{-2}) = \frac{6}{\pi^2}$$

(vedi LEZIONE 3 - TEOREMA DEI NUMERI PRIMI)

$$\text{MCD}(A, B) = 1 \Rightarrow \exists C, D \text{ t.c. } AD + BC = 1$$

$$\Rightarrow \det \begin{pmatrix} A & -B \\ C & D \end{pmatrix} = 1 \Rightarrow \begin{pmatrix} A & -B \\ C & D \end{pmatrix} \underbrace{\text{è unimodulare}}_{\text{VOCI INTERE}}$$

Si tratta di un algoritmo con complessità polinomiale,
ma funziona solo per matrici 2×2 .

DEF Sia H una matrice $n \times m$ con voci intere.

Allora H è in forma normale di Hermite se:

1) H è a scalimi (*)

2) Ogni pivot di H è un num. positivo

3) Se una colonna contiene un pivot, le voci sopra il pivot sono numeri interi non negativi strettamente inferiori al pivot

NOTA

$$\text{ES. 2)} \begin{pmatrix} 1 & 2 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \xrightarrow{R_2 = R_2 \cdot -1} \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \checkmark$$

$$\text{ES. 3)} \begin{pmatrix} 1 & 3 & 1 \\ 0 & 2 & 1 \\ 0 & 0 & 0 \end{pmatrix} \xrightarrow{R_1 = R_1 - R_2} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 0 \end{pmatrix} \checkmark$$

(*) $A \in \mathbb{N}^{n \times m} \rightarrow A \sim B$ se A e B hanno la stessa

forma canonica di riga
GESS-JORDAN (ogni pivot = 1, gli altri elem. nelle colonne pivot 0)

ma vale solo in $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ poiché per ottenere la forma canonica interviene la divisione, dunque non è detto si abbiano voci intere

TH Sia A una mat. $n \times m$ con voci intere.

Allora $\exists! H$ mat. in forma normale di Hermite

t.c. $H = UA$ per una qualche mat. unimodulare U

Possiamo quindi costruire matrici unimodulari casuali partendo da una matrice intera casuale A e calcolando la mat. in forma normale di Hermite $H = UA$. Ciò può essere fatto in tempo polinomiale tramite l'alg. di LENSINKA - LENSTRA - LOVASZ (LLL) -

Possiamo anche usare la forma normale di Hermite per determinare quando $L(B) = L(C)$:

Supponiamo che B^T e C^T abbiano la stessa forma normale H : $UB^T = H = VC^T$, U e V unimodulari

$$\Rightarrow BU^T = CV^T \Rightarrow B = \underbrace{CV^T(U^T)^{-1}}_{\text{MAT. UNIMODULARE}} \Rightarrow L(B) = L(C)$$

ALGORITMO DI LENSTRA - LENSTRA - LOVASZ (LLL)

L'algoritmo LLL è un analogo dell'algoritmo di Gauss che modifica il processo di Gram-Schmidt per produrre una base ridotta del reticolo, che consiste di vettori relativamente brevi, quasi ortogonali.
 (Nota: LLL non trova un vettore più corto)

DEF Una base (b_1, \dots, b_d) è (δ, γ) -LLL-ridotta se:

- $\forall i > j$ si ha $|\mu_{ij}| \leq \eta$
- $\forall i < d$ si ha $\delta |b_i^*|^2 \leq |b_{i+1}^* + \mu_{i+1,i} b_i^*|^2$

dove $\mu_{ij} = \frac{(b_i, b_j^*)}{(b_j, b_j^*)}$ e b_i^* è l' i -esimo vettore dell'ortogonalizz. di Gram-Schmidt di (b_1, \dots, b_d) .

I parametri δ e γ devono soddisfare $0.25 \leq \delta \leq 1$ e $0.5 \leq \gamma < \sqrt{\delta}$

Oltre a trovare la forma normale di Hermite di una matrice, un'altra applicazione dell'algoritmo LLL è la fattorizzazione dei polinomi.

In particolare, il problema di determinare se un polinomio con coeff. razionali ha una radice razionale ha complessità polinomiale.

ISOMETRIA

Un' isometria è una qualsiasi trasformazione geometrica definita nel piano o nello spazio che mantiene inalterate le caratteristiche misurabili di una figura (misure dei lati, ampiezze degli angoli, perimetro, area, volume).

Esempi di isometrie sono TRASLATORI, ROTAZIONI, AFFISSIONI.

ESEMPI

- 1) Due triangoli T_1 e T_2 sono congruenti se c'è un' isometria che sposta T_1 su T_2
- 2) Due rette L_1 e L_2 sono parallele se si può spostare L_1 su L_2 con una traslazione (considerando un sottoinsieme ristretto di isometrie)
- 3) Due triangoli T_1 e T_2 sono simili se T_1 diventa congruente a T_2 dopo avere scalato le distanze (ammettendo questa ulteriore trasformazione)

DEF (RELAZIONE)

Sia S un insieme.

Allora, una relazione R su S è un sottoinsieme del prodotto cartesiano $S \times S$.

Dati due elementi $a, b \in S$ diciamo che a è in relazione con b , scritto aRb , se $(a, b) \in R$.

Nota: aRb e $(a, b) \in R$ sono notazioni equivalenti per indicare che a è in relazione con b

ESEMPIO

4) $S = \mathbb{Z}$, $a R b \Leftrightarrow a \leq b$

cioé a è in relazione \leq con b quando $a \leq b$

5) Sia S un insieme e $P(S)$ l'insieme di tutti i sottoinsiemi di S .

Allora $(A, B) \in R \Leftrightarrow A \subseteq B$ è una relazione su $P(S)$

ES.

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

$$|P(S)| = 2^3 = 8$$

$$A R B \Leftrightarrow A \subseteq B$$

Una relazione R su un insieme finito $S = \{s_1, \dots, s_n\}$ può essere rappresentata dalla matrice booleana $n \times n$:

$$M = (m_{i,j}), \quad m_{i,j} = \begin{cases} 1 & (s_i, s_j) \in R \\ 0 & (s_i, s_j) \notin R \end{cases}$$

Equivalentemente, una relazione R può essere rappresentata da un grafo diretto (orientato) il cui insieme di vertici S presenta una freccia da s_i a $s_j \Leftrightarrow m_{i,j} = 1$, ovvero $(s_i, s_j) \in R$.

Se M è simmetrica allora $(s_i, s_j) \in R \Leftrightarrow (s_j, s_i) \in R$ e possiamo rappresentare R con un grafo non diretto. A seconda della def., un grafo può avere o meno un "self loop" da un vertice a sé stesso.

Nell'esempio sopra, un self loop da s_i a s_i corrisponde a $m_{ii} = 1$, che è consentito.

(SE $R \subset \mathbb{N} \text{ mat. } n \times n$, ALLORA R SIMM. $\Leftrightarrow M = M^T$)

DEF (RELAZIONE SIMMETRICA)

Una relazione su R è simmetrica se:

$$aRb \Rightarrow bRa \quad \forall (a, b) \in S \times S.$$

(**ANTISIMMETRICA** se $aRb \Rightarrow bRa$)

NOTA: gli esempi 1, 2, 3 sono relazioni simmetriche, così come congruenza e similitudine, gli es. 5, 6 no

DEF (RELAZIONE RIFLESSIVA)

Una relazione R su S è riflessiva se $aRa \quad \forall a \in S$

NOTA: tutti gli esempi sopra sono relazioni riflessive

ESEMPIO

6) Sia S un insieme arbitrario.

$$\text{Sia } R = \emptyset \subset S \times S.$$

$aRa \Rightarrow a \in R$, ma $R = \emptyset \nmid \Rightarrow R$ non è riflessiva

Se R è una relazione riflessiva su un insieme finito allora gli elementi diagonali della mat. corrispondente sono tutti 1.

7) Sia $S = \{2, 3, \dots\}$

$$aRb \Leftrightarrow \text{MCD}(a, b) = 1$$

$\text{MCD}(a, b) = \text{MCD}(b, a) \Rightarrow R$ è simmetrica

$\text{MCD}(a) = a > 1 \Rightarrow R$ non è riflessiva

DEF (RELAZIONE TRANSITIVA)

Una relazione R è transitiva $\Leftrightarrow aRb, bRc \Rightarrow aRc$

Se una mat. bool. M rappr. una relazione transitiva R allora $(M^2)_{ac} \neq 0 \Rightarrow M_{ac} \neq 0$

NOTA: tutti gli esempi sopra sono relazioni transitive, tranne il 7: infatti $\text{MCD}(2,3)=1$, $\text{MCD}(3,4)=1$, ma $\text{MCD}(2,4)=2$

DEF (RELAZIONE DI EQUIVALENZA) NOTAZIONE: $a \sim b$, $a \cong b$

Una relazione R su un insieme S è una relazione di equivalenza \Leftrightarrow è riflessiva, simmetrica e transitiva

NOTA: congruenza, parallelismo e similitudine (esempi 1, 2, 5) sono relazioni di equivalenza

DEF (ORDINE PARZIALE) NOTAZIONE: $a \leq b$

Una relazione R su un insieme S è un ordine parziale \Leftrightarrow è riflessiva, antisimmetrica e transitiva

NOTA: le relazioni \leq e \subseteq (esempi 4, 5) sono ordini parziali

NOTA: Sia M una mat. $n \times n$ booleana generata casualm.

In generale, la relazione associata R non è:

- RIFLESSIVA perché qualche voce diagonale $M_{ii} \neq 0$
- SIMMETRICA perché M non è simmetrica
- TRANSITIVA perché $(M^2)_{ac} \neq 0 \Rightarrow M_{ac} \neq 0$

ESEMPI

8) Sia S l'insieme di tutte le mat. $n \times m$.

Allora $A \sim B \Leftrightarrow A$ è equiv. per righe $\wedge B$ è una rel. di equivalenza

(due mat. sono equiv. per righe se hanno la stessa forma canonica)

9) Sia S l'insieme di tutte le mat. $n \times n$.

Allora $A \sim B \Leftrightarrow A$ è simile a B è una rel. di equivalenza (cioè se $A = PBP^{-1}$ per una qualche mat. $n \times n$ invertibile P , per la def. di mat. simile)

DIM

$$A \sim A \Rightarrow P = I \text{ rel. riflessiva} \checkmark$$

$$A \sim B \Rightarrow A = PBP^{-1} \Rightarrow P^{-1}AP = B \text{ rel. simmetrica} \checkmark$$

$$A \sim B, B \sim C \Rightarrow A = PBP^{-1}, B = QCQ^{-1} \Rightarrow A = PQCQ^{-1}P^{-1} = \\ = (PQ)C(PQ)^{-1} \text{ rel. transitiva} \checkmark$$

DEF (CLASSE DI EQUIVALENZA)

Sia \sim una relazione di equivalenza su S e $a \in S$.

Allora l'insieme $[a] = \{b \in S : a \sim b\}$ si chiama CLASSE DI EQUIVALENZA di a .

Un elemento $s \in S$ t.c. $s \sim a$ si chiama un RAPPRESENTANTE di $[a]$.

ESEMPIO

$A \in S, S = \{\text{matrici } n \times n\}$

$[A] = \{\text{matrici equiv. per righe ad } A\}$

LEMMA

Sia \sim una relazione di equivalenza sull'insieme S .

Siamo $[a]$ e $[b]$ due classi di equivalenza.

Allora $[a] = [b]$ oppure $[a] \cap [b] = \emptyset$

DIM

- $a, b \in S, aRb \Rightarrow [a] = [b]$

Sia $x \in [a]$, allora per la def. di classe di equiv. aRx

R rel. di equiv. $\Rightarrow R$ simmetrica $\Rightarrow aRb = bRa$

" " " " " $\Rightarrow R$ transitiva $\Rightarrow bRa, aRx \Rightarrow bRx$

$$\Rightarrow x \in [b]$$

Sia $x \in [b]$, allora bRx .

$$\Rightarrow bRa = aRb$$

$$\Rightarrow aRb, bRx \Rightarrow aRx$$

$$\Rightarrow x \in [a]$$

$$x \in [a] \Leftrightarrow x \in [b] \Rightarrow [a] = [b]$$

- Supponiamo $[a] \cap [b] \neq \emptyset$.

Allora $\exists x \in [a] \cap [b]$, quindi aRx, bRx

$$\Rightarrow bRx = xRb$$

$$\Rightarrow aRx, xRb \Rightarrow aRb$$

$\Rightarrow [a] = [b]$ e $[a] \cap [b]$ sono equivalenti

DEF (SPAZIO QUOTIENTE)

Sia \sim una relazione di equivalenza su S .

Allora S/\sim è l'insieme di tutte le classi di equivalenza di elementi di S .

L'insieme S/\sim è chiamato SPAZIO QUOTIENTE di S rispetto a \sim . (SI LEGGE ANCHE "S QUOTIENTE TILDE")

ESEMPIO

$$S = \{ \text{mat. } n \times m \}$$

\sim = equivalente per righe

$[A] \rightarrow$ forma canonica A'

$$A \sim B \Leftrightarrow A' = B'$$

$S/\sim = \{ \text{tutte le matrici } n \times m \text{ in forma canonica} \}$

ESEMPIO

$$S = \{ \text{mat. } 2 \times 2 \}$$

$$A \sim B \Rightarrow \text{rk}(A) = \text{rk}(B)$$

$$\text{rk}(A) = 2 \Rightarrow \text{la forma canonica di } A \text{ è } I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\text{rk}(A) = 1 \Rightarrow \begin{pmatrix} 1 & a \\ 0 & 0 \end{pmatrix}, a \in \mathbb{R}$$

$$\text{rk}(A) = 0 \Rightarrow \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

S/\sim

ESEMPIO

$$S = \{ \text{mat. } 2 \times 3 \}$$

$$A \sim B \Rightarrow \text{rk}(A) = \text{rk}(B)$$

$$\text{rk}(A) = 2 \Rightarrow \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & b \end{pmatrix}, \begin{pmatrix} 1 & a & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\text{rk}(A) = 1 \Rightarrow \begin{pmatrix} 1 & a & b \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

$$\text{rk}(A) = 0 \Rightarrow \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Per individuare lo spazio quoziente si puo' costruire una mappa $f: S \rightarrow T$ t.c.:

- $f(s) = T$
- $f(a) = f(b) \Leftrightarrow a \sim b$

Data una tale mappa f , possiamo definire una mappa $g: (S/\sim) \rightarrow T$ t.c.: $g([s]) = f(s)$

Per dim. che g e' ben definita supponiamo $s \sim s'$.

Allora $f(s) = f(s')$.

Dunque g dipende solo dalla classe di equivalenza $[s]$ al primo membro e non dal rappresentante s al secondo membro.

Poiché f e' suriettiva lo e' anche g .

$(f(s) = T \Rightarrow g(S/\sim) = T, f(s) = t \Rightarrow g([s]) = t)$.

Inoltre g e' iniettiva poiché:

$g([s]) = g([s']) \Rightarrow f(s) = f(s') \Rightarrow s \sim s'$ cioè $[s] = [s']$

ESEMPIO

Tornando all'esempio 8:

Sia S l'insieme di tutte le mat. $n \times m$.

Allora $A \sim B \Leftrightarrow A$ e' equiv. per righe a B e' una rel. di equivalenza.

Siamo $S = \{ \text{mat. } n \times m \}$, $T = \{ \text{mat. } n \times m \text{ in forma canonica} \}$

Allora l'eliminazione di Gauss-Jordan restituisce

una mappa suiettiva $f: S \rightarrow T$.

Inoltre, due mat. A e B sono equiv. per rechte \Leftrightarrow hanno la stessa forma canonica, ovvero:

$$f(A) = f(B) \Leftrightarrow A \sim B$$

Quindi la mappa $g: (S/\sim) \rightarrow T$ è biettiva

ESEMPIO

$$a \sim b \text{ su } \mathbb{Z} \Leftrightarrow a - b \in 2\mathbb{Z}$$

$$[0] = 2\mathbb{Z} \text{ perché } a - 0 \text{ pari} \Rightarrow a \text{ pari}$$

$$[1] = 1 + 2\mathbb{Z} \text{ perché } a - 1 \text{ pari} \Rightarrow a \text{ dispari}$$

$$\mathbb{Z}/\sim = \{[0], [1]\}$$

ESEMPIO

$$a \in \mathbb{C}, a \sim b \Leftrightarrow |a| = |b|$$

\sim è una rel. di equivalenza perché:

- $|a| = |a| \checkmark$
- $|a| = |b| \Rightarrow |b| = |a| \checkmark$
- $|a| = |b|, |b| = |c| \Rightarrow |a| = |c| \checkmark$

$$\mathbb{C}/\sim = [0, \infty[$$

ESEMPIO

Sia P l'insieme di tutte le permutazioni di $\{1, \dots, n\}$.

Allora:

$$(z_1, \dots, z_n) \sim (w_1, \dots, w_n) \Leftrightarrow \exists \sigma \in P \text{ t.c. } z_j = w_{\sigma(j)} \text{ per } j=1, \dots, n$$

definita su $S = \mathbb{C}^n$ è una rel. di equivalenza su \mathbb{C}^n .

Sia $T \subseteq \mathbb{C}[\lambda]$ l'insieme dei polinomi monici di grado n nella variabile λ .

Allora:

- $f: S \rightarrow T, f(z_1, \dots, z_n) = (\lambda - z_1)(\lambda - z_2) \dots (\lambda - z_n)$

è suiettiva perché $p \in T \Rightarrow p = t^n + \dots + a_0 = (t - z_1) \dots (t - z_n)$

cioè un polinomio monico di grado n si può fattorizzare in un prodotto di quella forma per il fondamentale teorema dell'algebra.

Il valore di $f(z_1, \dots, z_n)$ non varia con le permutazioni di (z_1, \dots, z_n) .

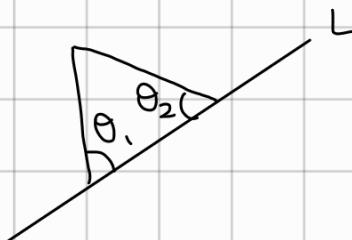
$$\cdot f(z) = f(w) \Leftrightarrow z \sim w$$

perché la fatt. di un polinomio monico $p(x)$ i fattori lineari della forma $(x-a)$ è unica fino al riordinamento dei fattori.

ESEMPIO

S = insieme dei triangoli nel piano

\sim = congruenza (rel. di equivalenza)



L = retta nel piano

$\Delta \in S$ e ha lati $\lambda_1 \leq \lambda_2 \leq \lambda_3$

1) $\lambda_1 = \lambda_2 = \lambda_3 \Rightarrow$ attraverso un movimento rigido si pone uno qualsiasi dei lati di Δ su L

2) $\lambda_2 < \lambda_3 \Rightarrow$ Si pone il lato più lungo (λ_3) su L

$$\lambda = \lambda_3$$

3) $\lambda_1 < \lambda_2 \Rightarrow$ Si pone il lato più corto (λ_1) su L

$$\lambda = \lambda_1$$

PERCHÉ LA RIFLESS. RISPETTO
A UNA RETTA + A L È UNA
CONGRUENZA

$$T = \{(\theta_1, \theta_2, \lambda) \in (0, \pi), (0, \pi), (0, \infty) : \theta_1 \leq \theta_2, \theta_1 + \theta_2 < \pi\}$$

Allora, il processo descritto definisce una mappa

$$f: S \rightarrow T$$

$$\Delta_1 \sim \Delta_2 \Leftrightarrow f(\Delta_1) = f(\Delta_2)$$

Finche $\theta_1 + \theta_2 < \pi$, dato un pto im Γ possiamo costruire un triangolo con le seguenti proprietà:

Sceglieremo un semipiano H su un lato di L e disegneremo su H i raggi che partono dai vertici dati, formano gli angoli dati con L e sono diretti verso l'altro vertice.

$\theta_1 + \theta_2 < \pi \Rightarrow$ i due raggi si intersecano

ESEMPIO

$S =$ insieme delle rette im \mathbb{R}^2

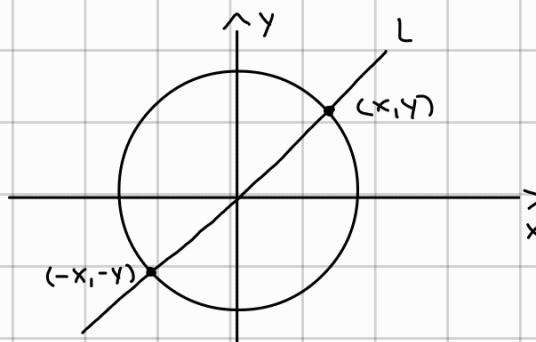
$\sim =$ traslazione

$l_1 \sim l_2 \Leftrightarrow l_1 \parallel l_2$

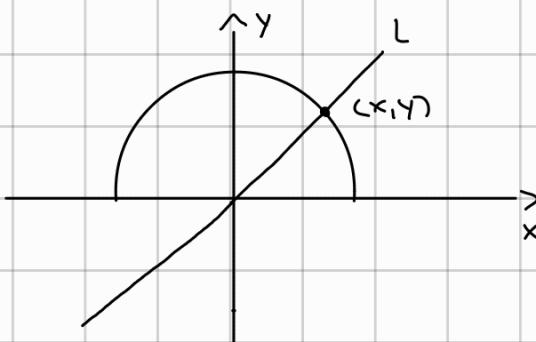
Ogni retta $l \in S$ è equiv. a una retta L che passa per l'origine.

Sia C il cerchio unitario dato dall'equazione $x^2 + y^2 = 1$.

Allora, una retta L che passa per l'origine interseca C nei punti (x, y) e $(-x, -y)$.

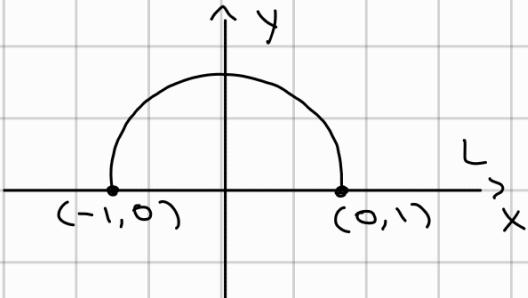


Sia c il sottoinsieme di C costituito dai punti per cui $y \geq 0$.



Allora, a meno che L non sia l'asse x , $L \cap C'$ è un singolo punto (x, y) con $y > 0$.

Se L è l'asse x invece $L \cap C' = \{(-1, 0), (0, 1)\}$



Sia $T = C' - \{(-1, 0)\}$.

Allora $L \cap T$ è sempre costituito da un singolo punto p da cui si può riconoscere L come la retta che attraversa l'origine e interseca la semicirconferenza in p .

In questo modo otteniamo:

- $f: S \rightarrow T = [0, \infty[$ mappa suriettiva
- Per costruzione $f(L) = f(L') \Leftrightarrow L \parallel L'$ cioè se $L \sim L'$

DEF

Sia S un insieme.

Allora, una partizione di S è una collezione di sottoinsiemi \mathcal{P} di S t.c.:

- $s \in S \Rightarrow \exists A \in \mathcal{P}$ t.c. $s \in A$
- $A, B \in \mathcal{P} \Rightarrow A = B$ oppure $A \cap B = \emptyset$

(cioè: una partizione di S è una decomposizione di S in una collezione di sottoinsiemi mutualmente disgiunti)

ESEMPIO

Sia P una partizione dell'insieme S .

Allora, $a \sim b \Leftrightarrow \exists P \in P \text{ t.c. } a, b \in P$ è una rel. di equivalenza su S .

DIM

- $S = \bigcup_{A \in P} A \Rightarrow a \sim a$ perché $\exists A \text{ t.c. } a \in A$

- $a \sim b \Rightarrow a, b \in A \Rightarrow b, a \in A \Rightarrow b \sim a$

- $a \sim b, b \sim c$

$$a, b \in P_1, b, c \in P_2$$

$$\Rightarrow b \in P_1 \cap P_2$$

$$P_1 \cap P_2 \neq \emptyset \Rightarrow P_1 = P_2 \Rightarrow a, c \in P_1 = P_2 \Rightarrow a \sim c$$

ESEMPIO

Sia \sim una relazione di equivalenza su S .

Allora, $P = \{[a] : a \in S\}$ è una partizione di S .

DIM

- $S = \bigcup [a]$ (cioé S è l'unione di tutte le classi di equiv.)
 $s \in S \Rightarrow s \sim s \Rightarrow s \in [s]$

- $[a] \cap [b] = \begin{cases} [a] = [b] \\ \emptyset \end{cases}$

$$c \in [a] \cap [b] \Rightarrow a \sim c, b \sim c$$

$$\begin{matrix} \parallel & \text{PER SIMMETRIA} \\ \vee & \\ c \sim b & \end{matrix}$$

$$a \sim c, c \sim b \Rightarrow a \sim b \Rightarrow [a] = [b]$$

TH

Si fissi un insieme S .

Sia $\Pi = \{ \text{tutte le possibili partizioni di } S \}$

Sia $\mathcal{E} = \{ \text{tutte le possibili relazioni di equivalenza su } S \}$

Si denoti con $f: \Pi \rightarrow \mathcal{E}$ la mappa definita da

$a \sim b \Leftrightarrow \exists P \in \Pi \text{ t.c. } a, b \in P$ (E_1)

Si denoti con $g: \mathcal{E} \rightarrow \Pi$ la mappa definita da

$P = \{[a] : a \in S\}$ (E_2)

Allora $f \circ g$ e $g \circ f$ sono le mappe identità rispettivamente su \mathcal{E} e Π .

In altre parole, f e g sono bijetioni inverse.

DIM

• $f \circ g = \text{Id}_{\mathcal{E}}$

Sia $P = g(\sim)$ e $R = f(P)$.

Dobbiamo dim. che $aRb \Leftrightarrow a \sim b$

i) Supponiamo $a \sim b$

$$\stackrel{E_2}{\Rightarrow} \exists P \in \Pi \text{ t.c. } a, b \in P$$

$$\stackrel{E_1}{\Rightarrow} aRb$$

$$\text{Cioè } a \sim b \Rightarrow aRb$$

ii) Viceversa supponiamo aRb .

$$\stackrel{E_1}{\Rightarrow} \exists P \in \Pi \text{ t.c. } a, b \in P$$

$$\stackrel{E_2}{\Rightarrow} a \sim b$$

• $g \circ f = \text{Id}_{\Pi}$

Sia $R = f(P)$ e $P' = g(R)$

Allora, poiché P e P' sono partizioni di S , dato $s \in S$

$\exists A \in P$ e $\exists B \in P'$ che contengono s .

Dobbiamo dim. che $A = B$

i) $A \subseteq B$

Supponiamo $s' \in A$

$$\stackrel{E_1}{\Rightarrow} sR s'$$

$$\stackrel{E_2}{\Rightarrow} s' \in B$$

ii) $B \subseteq A$

Supponiamo $s' \in B$

$$\stackrel{E_2}{\Rightarrow} s' R s$$

$$\stackrel{E_1}{\Rightarrow} s' \in A$$

□

NOTE

Mappa identità su Σ : $\forall x \in \Sigma \quad id_{\Sigma}(x) = x$

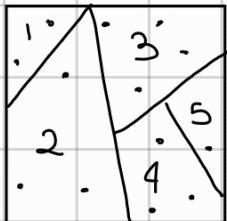
" " " su Π : $\forall x \in \Pi \quad id_{\Pi}(x) = x$

cioè la mappa identità associa ad ogni elem. l'elem. stesso

Il th implica che c'è un rapporto 1 a 1 tra partizione e rel. di equivalenza, cioè: da una partizione ottengo una rel. di equiv. e viceversa.

ESEMPIO (PARTIZIONE \rightarrow RELAZIONE)

S:



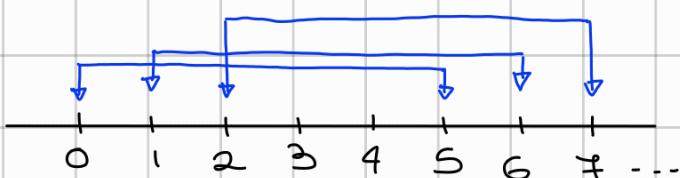
$[1] \cup [2] \cup [3] \cup [4] \cup [5]$ è una partiz. dis
(o meglio, l'unione dei punti costituisce
una partizione di S)

$$a \sim b \Leftrightarrow U_a \cap U_b = \emptyset \text{ per } a \neq b$$

è una relazione di equivalenza

ESEMPIO (RELAZIONE \rightarrow PARTIZIONE)

$$a \sim b \Leftrightarrow 5 | a - b \text{ è una rel. di equivalenza}$$



$$5 \sim 0 \Leftarrow 5|5$$

$$6 \sim 1 \Leftarrow 5|(6-1)$$

$$7 \sim 2 \Leftarrow 5|(7-2)$$

$$8 \sim 3 \Leftarrow 5|(8-3)$$

$$9 \sim 4 \Leftarrow 5|(9-4)$$

...

$$\mathbb{Z}/\sim = \{[0], [1], [2], [3], [4]\}$$

$$\begin{aligned} P &= \{5n : n \in \mathbb{Z}\} \cup \{5n+1 : n \in \mathbb{Z}\} \cup \{5n+2 : n \in \mathbb{Z}\} \\ &\quad \cup \{5n+3 : n \in \mathbb{Z}\} \cup \{5n+4 : n \in \mathbb{Z}\} = \\ &= [0] \cup [1] \cup [2] \cup [3] \cup [4] \end{aligned}$$

P è una partizione

SPAZI VETTORIALI QUOTIENTI

COSTRUTTONE DI UNO SPAZIO VETTORIALE QUOTIENTE (SU \mathbb{R}^n):

Sia \sim la relazione su \mathbb{R}^n definita dalla condizione che $x \sim y \iff$ le ultime k coordinate di x e y sono le stesse.

Per dimostrare che \sim è una relazione di equivalenza si possono verificare direttamente gli assiomi oppure sia $\pi: \mathbb{R}^n \rightarrow \mathbb{R}^k$ la mappa lineare data la proiezione sulle ultime k coordinate.

In questo caso \sim è semplicemente la relazione di equivalenza associata a π :

- $\pi(\mathbb{R}^n) = \mathbb{R}^k$ cioè π è suriettiva
- $\pi(x) = \pi(y) \iff x \sim y$

Per rendere questa costruzione indipendente dalle coordinate, sia U il sottospazio di \mathbb{R}^n costituito dai vettori x per cui le ultime k coordinate sono zero, dunque $U = \ker(\pi)$. Allora $x \sim y \iff x - y \in U$

- $x \sim y \Rightarrow$ le ultime k coordinate di x e y sono le stesse e quindi $x - y \in U$
- $u = x - y \in U \Rightarrow x = u + y$, dove le ultime k coordinate di u sono zero.

Allora, le ultime k coordinate di x e y sono identiche e quindi $x \sim y$

Possiamo ora estendere questa costruzione a spazi vettoriali arbitrari.

LEMMA

Sia U un sottospazio di V .

Allora, $x \sim y \Leftrightarrow x - y \in U$ è una rel. di equiv. su V (*)

DIM

- **RIFLESSIVITÀ:** $x \in V \Rightarrow x - x = 0 \in U \Rightarrow x \sim x$
- **SIMMETRIA:** $x, y \in V, x \sim y \Rightarrow x - y = u \in U \Rightarrow y - x = -u \in U \Rightarrow y \sim x$
- **TRANSITIVITÀ:** $x, y, z \in V \Rightarrow x - z = (x - y) + (y - z) \in U$
poiché $x \sim y \Rightarrow x - y \in U$ e $y \sim z \Rightarrow y - z \in U$
 $\Rightarrow x \sim z$

□

NOTA: lo spazio quoziente di V definito dalla rel. di equiv.

(*) si denota con V/U

LEMMA

Sia U un sottospazio di V .

Allora V/U è uno spazio vettoriale rispetto alle operazioni

- $c[v] = [cv]$
- $[v] + [v'] = [v + v']$

(dove $[v], [v'] \in V/\sim (= V/U)$)

DIM (verifichiamo che le op. siano ben definite)

$$x \sim y \Rightarrow x - y \in U$$

$$\bullet c x = c(y + x - y) = cy + c(x - y) \Rightarrow cx \sim cy$$

$\Rightarrow [cx] = [c[x]]$ è ben definita perché $x - y \in U$

$$\bullet [v] + [v'] = [v + v']$$

$$x_1 \sim x_2 \Rightarrow x_1 - x_2 \in U$$

$$y_1 \sim y_2 \Rightarrow y_1 - y_2 \in U$$

$$x_1 + y_1 \sim x_2 + y_2 \Rightarrow (x_1 + y_1) - (x_2 + y_2) \in U$$

$$\text{perché } (x_1 + y_1) - (x_2 + y_2) = \underbrace{(x_1 - x_2)}_{\in U} + \underbrace{(y_1 - y_2)}_{\in U} \in U$$

□

Siamo U e W sottospazi di uno spazio vettoriale V .

Ricordiamo che:

- $U+W$ è il più piccolo sottospazio di V che contiene $U \cup W$
(cioè consiste di tutti gli elem. im V della forma
 $v = u + w$, $u \in U$, $w \in W$)
- $V = U \oplus W$ se $U+W = V$ e $U \cap W = \{0\}$
In questo caso, ogni elem. v ha un'unica rapp.
come $v = u + w$, $u \in U$, $w \in W$

PROPOSIZIONE

$V = U \oplus W \Rightarrow V/U$ è isomorfo a W attraverso la mappa
 $f([v]) = w$, $v = u + w$, $u \in U$, $w \in W$

DIM

Dim. immostreremo che f è ben definita.

$V = U + W \Rightarrow$ ogni vettore può essere scritto come una somma $v = u + w$, $u \in U$, $w \in W$

Supponiamo che $v = u' + w'$ sia un'altra rapp. di v .

Allora:

$$v = u + w = u' + w' \Rightarrow u - u' = w - w' \in U \cap W = \{0\} \Rightarrow u = u', w = w'$$

$\Rightarrow f([v]) = w$ è ben definita

f è una mappa lineare perché:

- $f([v_1] + [v_2]) = f([v_1]) + f([v_2]) = w_1 + w_2$
- $f([cv]) = c f([v]) = cw$

$w \in W \Rightarrow f([w]) = w$ e quindi $f: V/U \rightarrow W$ è suriettiva

Rimane da dim. che f è iniettiva.

Supponiamo $f([v]) = 0$ e scriviamo $v = u + w$, $u \in U$, $w \in W$.

Allora $f([v]) = w = 0$ e quindi $v \in U$.

$$\Rightarrow [v] = 0$$

□

Un metodo standard per trovare una decomposizione come somma diretta $V = U \oplus W$ è attraverso operatori di proiezione:

DEF (OPERATORE DI PROIEZIONE)

Un endomorfismo $\pi: V \rightarrow V$ è chiamato OPERATORE DI PROIEZIONE se $\pi^2 = \pi$.

Se U è un sottospazio di V allora un operatore di proiezione su U è un operatore di proiezione t.c. $\pi(V) = U$

LEMMA

Sia $\pi: V \rightarrow V$ un operatore di proiezione.

Sia $U = \pi(V)$ e $W = \text{Ker}(\mathbb{I} - \pi)$ dove $\mathbb{I}: V \rightarrow V$ è la mappa identità.

Allora, $V = U \oplus W$

DIM

Sia $v \in V$.

$$\Rightarrow v = \pi(v) + (\mathbb{I} - \pi)(v) \text{ dove } \pi(v) \in U \text{ e } (\mathbb{I} - \pi(v)) \in W$$

$$\Rightarrow v \in U + W \text{ e quindi } V = U + W$$

Supponiamo $t \in U \cap W$.

Allora, $t \in U \Rightarrow t = \pi(v)$ per un qualche $v \in V$

Allo stesso modo, $t \in W \Rightarrow t = (\mathbb{I} - \pi)(v')$ per un qualche $v' \in V$

Allora:

$$\cdot \pi^2 = \pi, t = \pi(v) \Rightarrow \pi(t) = \pi(\pi(v)) = \pi(v) = t$$

$$\cdot \pi^2 = \pi, t = (\mathbb{I} - \pi)(v') \Rightarrow \pi(t) = \pi(\mathbb{I} - \pi)(v') - \pi^2(v') = 0$$

$$\Rightarrow t = 0$$

□

Sia $(*,*)$ un prodotto scalare (o hermitiano) su uno spazio vettoriale reale (o complesso) V e sia U un sottospazio di V .

Allora $U^\perp = \{v \in V : (v, u) = 0 \forall u \in U\}$ è chiamato **COMPLEMENTO ORTOGONALE** di U .

Ricordiamo che per il processo di Graham-Schmidt, se U ha dim. finita, possiamo costruire una base ortonormale (o unitaria) $B = \{u_1, \dots, u_n\}$ t.c. $(u_i, u_j) = \delta_{ij}$

PROPOSIZIONE

Sia $(*,*)$ un prodotto scalare (o hermitiano) su uno spazio vettoriale reale (o complesso) V .

Sia U un sottospazio di dim. finita di V con base ortonormale (o unitaria) $B = \{u_1, \dots, u_n\}$.

Allora

$$\pi_U(v) = \sum_{j=1}^n (v, u_j) u_j$$

è un operatore di proiezione con immagine U .

DIM

- $\pi_U(V) = U$

Per def. $v \in V \Rightarrow \pi_U(v)$ è una combinazione lineare dei vettori della base B e quindi $\pi_U(v) \subseteq U$.

Viceversa, poiché B è una base ortonormale (o unitaria) di U :

$$\pi_U(u_k) = \sum_{j=1}^n (u_k, u_j) u_j = u_k$$

e quindi $u = \sum_{j=1}^n c_j u_j \in U \Rightarrow \pi_U(u) = u$
 $\Rightarrow U \subseteq \pi_U(V) \Rightarrow \pi_U(V) = U$

- Si scriva $\pi(v) = \sum_{j=1}^n c_j u_j$

$$\Rightarrow \pi^2(v) - \pi(v) = \pi\left(\sum_{j=1}^n c_j u_j\right) - \sum_{j=1}^n c_j u_j =$$

$$= \sum_{j=1}^n c_j \pi(u_j) - \sum_{j=1}^n c_j u_j =$$

$$= \sum_{j=1}^n c_j u_j - \sum_{j=1}^n c_j u_j = 0$$

□

Siamo $n, a, b \in \mathbb{Z}$, $n > 1$.

Allora $a \equiv b \pmod{n} \Leftrightarrow n | a - b$

\downarrow
CONSEQUENTE

LEMMA $\equiv \pmod{n}$ è una rel. di equivalenza su \mathbb{Z}

DIM

- $a \equiv a \pmod{n}$ perché $a - a = 0 \in n | 0$
- $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$ perché $n | (a - b) \Rightarrow n | (b - a)$
- $a \equiv b \pmod{n} \Rightarrow n | (a - b)$, $b \equiv c \pmod{n} \Rightarrow n | (b - c)$
 $\Rightarrow n | (a - c)$ perché $a - c = (a - b) + (b - c)$
 $\Rightarrow a \equiv c \pmod{n}$

□

LEMMA

Sia \mathbb{Z}_n lo spazio quoziente di \mathbb{Z} rispetto a $(\equiv \pmod{n})$.

Sia $T = \{[0], \dots, [n-1]\}$.

Allora $f: \mathbb{Z} \rightarrow T$ definita da $f(a) = [a]$ definisce una bijetione da \mathbb{Z}_n a T .

DIM

Supponiamo $a, b \in \{0, \dots, n-1\}$ e $a \equiv b \pmod{n}$

Scambiamo a e b se necessario, assumiamo $a \geq b$

Allora $a \equiv b \pmod{n} \Rightarrow n | (a - b) \in \{0, \dots, n-1\} \Rightarrow a - b = 0 \Rightarrow a = b$

Per il th della divisione, dato $a \in \mathbb{Z}$ $\exists! (q, r) \text{ t.c.}$

$$a = qn + r, \quad 0 \leq r < n$$

Definiamo $f: \mathbb{Z} \rightarrow T$ tramite $f(a) = [a]$, allora:

- $f(\mathbb{Z}) = T$
- $f(a) = f(b) \Leftrightarrow a \equiv b \pmod{n}$

- La proposizione $f(\mathbb{Z}) = T$ è vera perché:

$$j \in \{0, \dots, n-1\} \Rightarrow f(j) = [j]$$

- Supponiamo $f(a) = f(b) = [r]$.

Allora $a = nq + r$, $b = nq' + r$ con $q, q' \in \mathbb{Z}$, quindi:

$$a - b = n(q - q') \Rightarrow a \equiv b \pmod{n}$$

Viceversa, $a \equiv b \pmod{n} \Rightarrow n \mid (a - b)$

$$\Rightarrow \exists c \text{ t.c. } a - b = nc$$

Sia $b = nq + r$, $0 \leq r < n$, allora:

$$a = a - b + b = nc + nq + r = n(c + q) + r$$

$$\Rightarrow f(a) = f(b)$$

□

DEF

Sia $[a], [b] \in T$. Allora,

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

NOTA: Dati $a, b \in \{0, \dots, n-1\}$, $a+b$ ($\circ ab$) potrebbe essere $>n$

In questo caso dobbiamo scrivere $a+b = qn+r$

($\circ ab = qn+r$) dove $0 \leq r < n$ e definiamo $[a+b] = [r]$

($\circ [ab] = [r]$).

LEMMA

Supponiamo che $a \equiv a' \pmod{n}$, $b \equiv b' \pmod{n}$.

Allora $a+b \equiv a'+b' \pmod{n}$, $ab = a'b' \pmod{n}$

DIM

$$\bullet \quad a \equiv a' \pmod{n}, b \equiv b' \pmod{n} \Rightarrow a+b \equiv a'+b' \pmod{n}$$

$$a \equiv a' \pmod{n} \Rightarrow a - a' = nq, q \in \mathbb{Z} \Rightarrow a = a' + nq$$

$$b \equiv b' \pmod{n} \Rightarrow b - b' = nr, r \in \mathbb{Z} \Rightarrow b = b' + nr$$

$$(a+b) - (a'+b') = a' + nq + b' + nr - a' - b' = \underbrace{n(q+r)}_{\text{MULTIPLO DI } n}$$

$$\Rightarrow a+b \equiv a'+b' \pmod{n}$$

$$\bullet \quad a \equiv a' \pmod{n}, b \equiv b' \pmod{n} \Rightarrow ab \equiv a'b' \pmod{n}$$

$$a \equiv a' \pmod{n} \Rightarrow a = a' + ns, s \in \mathbb{Z}$$

$$b \equiv b' \pmod{n} \Rightarrow b = b' + nt, t \in \mathbb{Z}$$

$$\Rightarrow ab = (a' + ns)(b' + nt) = a'b' + \underbrace{a'nt + nsb' + n^2st}_{\text{MULTIPLO DI } n}$$

$$\Rightarrow ab \equiv a'b' \pmod{n}$$

[OPPURE, PER TRANSPARENZA' (\equiv È UNA REL. DI EQUIV.)]

$$a \equiv a' \pmod{n} \Rightarrow ab \equiv a'b \pmod{n} \quad (\text{Moltiplico per } b \text{ entro i membri})$$

$$b \equiv b' \pmod{n} \Rightarrow a'b \equiv a'b' \pmod{n} \quad (" " " a' " " ")$$

$$\Rightarrow ab \equiv a'b' \pmod{n}$$

□

NOTA: Questo lemma implica che possiamo usare ogni scelta di rappresentanti per effettuare addizione e moltiplicazione mod n

ESEMPI

i) $\underbrace{[6][\frac{x}{2}]}_{42 = 40 + 2} \equiv x \pmod{4}$
 $42 = 40 + 2 \equiv 2 \pmod{4} \Rightarrow x = 2$

$\underbrace{[6][\frac{x}{9}]}_{42 = 36 + 6} \equiv x \pmod{9}$
 $42 = 36 + 6 \equiv 6 \pmod{9} \Rightarrow x = 6$

ii) $3x \equiv 5 \pmod{7}$

$[3][1] \equiv [3] \pmod{7}$

$[3][2] \equiv [6] \pmod{7}$

$[3][3] \equiv [2] \pmod{7}$

$[3][4] \equiv [5] \pmod{7} \Rightarrow x = 4$

$3x \equiv 2 \pmod{4}$

$[3][1] \equiv [3] \pmod{4}$

$[3][2] \equiv [2] \pmod{4} \Rightarrow x = 2$

iii) $2x \equiv 3 \pmod{4}$ mom l'ha una soluzione

(è sufficiente guardare la tabella della molt.
 $\pmod{4}$ per vedere che $\exists x$ t.c. $[2][x] \pmod{4} = [3]$)

TH (RECIPROCOITÀ QUADRATICA, GAUSS)

Siamo p e q due num. primi distinti dispari.

- $q \equiv 1 \pmod{4} \Rightarrow x^2 \equiv p \pmod{q}$ l'ha soluzione $\Leftrightarrow x^2 \equiv q \pmod{p}$ l'ha soluzione
- $q \equiv 3 \pmod{4}, p \equiv 3 \pmod{4} \Rightarrow x^2 \equiv p \pmod{q}$ l'ha soluzione
 $\Leftrightarrow x^2 \equiv -q \pmod{p}$ l'ha soluzione

PROPOSIZIONE (I SUPPLEMENTO ALLA RECIPROCA QUADRATICA)

$x^2 \equiv -1 \pmod{p}$ ha soluzione $\Leftrightarrow p \equiv 1 \pmod{4}$

Possiamo anche considerare sistemi lineari (A|b) usando l'aritmetica mod n.

Per la regola di Cramer, se A è una mat. quadrata allora $Ax \equiv b \pmod{n}$ ha soluzione perché possiamo risolvere l'equazione $[S][\det(A)] \equiv 1 \pmod{n}$.

(vedi esempio (1.15) lezione 7)

DEF (ANELLO COMMUTATIVO CON IDENTITÀ)

Un anello commutativo con identità è un insieme R con delle mappe:

$$+: R \times R \rightarrow R$$

$$*: R \times R \rightarrow R$$

che soddisfano le seguenti proprietà

TABLE 1. Proprietà di Addizione e Moltiplicazione, $a, b, c \in \mathbb{Z}$

	Addizione	Moltiplicazione
Chiusura	$a + b \in \mathbb{Z}$	$a * b \in \mathbb{Z}$
Associatività	$a + (b + c) = (a + b) + c$	$(ab)c = a(bc)$
Commutatività	$a + b = b + a$	$a * b = b * a$
Elementi Identità 1, 0	$a + 0 = a$	$a * 1 = a$
Esistenza di Inversi	$a + (-a) = 0$? (DI SOLITO NO)
Proprietà distributiva	$a * (b + c) = a * b + a * c$	

perché $\underline{1} \neq 0$

↳ FUNZIONE IDENTITÀ

ESEMPI (di anelli confe. con identità): $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_n$

ESEMPIO

Sia R un anello comm. con id.

Allora, possiamo definire l'anello polinomiale $R[x]$ come l'insieme di elementi (polinomi) della forma:

$$f(x) = a_n x^n + \dots + a_0, \text{ con } a_n, \dots, a_0 \in R$$

\curvearrowright VALUTAZIONE DELLA FUNZIONE

$f \in R[x]$ definisce $\overbrace{\text{ev}(f)}^{} : R \rightarrow R$

N.B.:

$$|R| < \infty \Rightarrow |\{f : R \rightarrow R\}| < \infty$$

Poiché R ha almeno due elementi ($0 \neq 1$), $|R[x]| = \infty$

Dunque $R[x] \neq$ funzione polinomiale

ES: \mathbb{Z}_2

$$|\{f : \mathbb{Z}_2 \rightarrow \mathbb{Z}_2\}| = 2^2 = 4 \quad \text{perché } f(0) = 0, 1 \text{ e } f(1) = 1, 0 \\ \Rightarrow 4 \text{ possibilità}$$

mentre

$$\mathbb{Z}_2[x] = \{a_n x^n + \dots + a_0 : n = 0, 1, \dots \text{ e } a_n, \dots, a_0 \in \mathbb{Z}_2\}$$

$$|\mathbb{Z}_2[x]| = \infty$$

ESEMPIO

Se $(R, +, *)$ e $(S, +, *)$ sono anelli comm. con id.

allora S è un anello comm. con id. rispetto all'addizione e alla moltiplicazione:

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$$

$$(r_1, s_1) \cdot (r_2, s_2) = (r_1 r_2, s_1 s_2)$$

ELEM. IDENTITÀ PER L'ADDITIONE: $(0_R, 0_S)$

$\sim \quad \sim \quad \sim \quad$ LA MOLTIPLIC.: $(1_R, 1_S)$

ESEMPIO

Siamo m, n interi > 1 .

CLASSE DI EQUIV.
↑ DI $x \bmod n$

Siamo $x \in \mathbb{Z}$, $[x]_{mn}$, $[x]_m$, $[x]_n$

Allora:

$f: \mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$, $f([x]_{mn}) = ([x]_m, [x]_n)$

è una mappa ben definita t.c.:

- $f([x+y]_{mn}) = f([x]_{mn}) + f([y]_{mn})$ → COME LA PROPRIETÀ DI SOMMA PER LE MAPPE LIN.
- $f([x]_{mn}[y]_{mn}) = f([x]_{mn})f([y]_{mn})$ → SIMILE AL PROD. SCALARE PER LE MAPPE LIN.

DIM (che f è ben definita)

Supponiamo $x \equiv x' \bmod mn$:

$$\Rightarrow x' = x + \alpha mn$$

$$\Rightarrow [x']_m = [x]_m \quad (\text{perché } m | \alpha mn)$$

$$[x']_n = [x]_n \quad (\text{perché } n | \alpha mn)$$

$$f([x]_{mn}) = f([x]_m, [x]_n) = f([x']_m, [x']_n) = f([x']_{mn})$$

Lo stesso vale per y .

□

Una grande differenza tra \mathbb{Z} e \mathbb{Z}_n è la possibile esistenza di divisori di 0.

Infatti:

$$\text{Su } \mathbb{Z}: ab = 0 \Rightarrow a = 0 \text{ oppure } b = 0$$

$\begin{matrix} 0 \\ \times \\ \times \end{matrix}$

$$\text{Su } \mathbb{Z}_n \text{ (supponendo } n \text{ non primo}): n = ab \Rightarrow [a][b] = [0]$$

$$\text{es su } \mathbb{Z}_6: [2][3] = [6] = [0] \text{ perché } 6 \bmod 6 = 0$$

□

DEF (DOMINIO DI INTEGRAZIONE)

Un dominio di integrità è un anello comm. com id.

t.c. $ab = 0 \Rightarrow a = 0$ oppure $b = 0$

ESEMPIO

- $\mathbb{Q}[x]$ è un dominio di integrità
(se entrambi due polinomi sono $\neq 0$ anche il loro prodotto è $\neq 0$)
- $R[x]$ non è un dominio di integrità perché (es.):

$$\underbrace{(1_R, 0_S)}_{\neq 0} \cdot \underbrace{(0_R, 1_S)}_{\neq 0} = \underbrace{(0_R, 0_S)}_{= 0}$$

DEF (UNITÀ, INVERSO MOLTIPLICATIVO)

Sia $(R, +, *)$ un anello comm. con id.

Allora, un elemento non nullo $u \in R$ è un'unità se $\exists v \in R$ t.c. $uv = 1$ (cioè se u ha un inverso mult.)

ESEMPI

In \mathbb{Z} le unità sono $\{\pm 1\}$

In $\mathbb{Q}[x]$ sono $\{a_0 : a_0 \neq 0\}$ cioè gli scalari non nulli
(se $\deg(f \in \mathbb{Q}[x]) > 1 \Rightarrow f$ non ha un inverso mult.)

LEMMA

$[a] \in \mathbb{Z}_n$ ha un inverso moltiplicativo $\Leftrightarrow \text{MCD}(a, n) = 1$

DIM

- Supponiamo $[a][b] = 1$ (cioè $ab \bmod n = 1$)
 $\Rightarrow \exists c \in \mathbb{Z}$ t.c. $ab = \underline{cn} + 1$
↳ RESTAURE SCARICO DI n
- $\Rightarrow ab + (-c)n = 1 \Rightarrow \text{MCD}(a, n) = 1$
- Viceversa, supponiamo $\text{MCD}(a, n) = 1$
 $\Rightarrow \exists b, c \in \mathbb{Z}$ t.c. $ab + cn = 1 \Rightarrow [a][b] = 1$

□

Corollario

Sia p un num. primo.

Allora, ogni elemento non nullo im \mathbb{Z}_p ha un inverso moltiplicativo (ovvero ogni elem. non nullo è un' unità).

DIM

Se $a \in \{1, \dots, p-1\}$ e p è primo, allora $\text{MCD}(a, p) = 1$

DEF (FUNZIONE DI EULERO)

La funzione $\phi : \mathbb{N}^* \rightarrow \mathbb{N}^*$ (dove $\mathbb{N}^* = \{1, 2, \dots\}$ è l' insieme degli interi positivi) definita come segue:

- $\phi(1) = 1$
- $\phi(n) = \#$ di unità im \mathbb{Z}_n

è chiamata funzione di Euler.

ESEMPIO

p primo $\Rightarrow \phi(p) = p-1$ (per il corollario proc.)

Più in generale, se r è un intero positivo:

$$\phi(p^r) = p^{r-1}(p-1) = p^r \left(1 - \frac{1}{p}\right), p \text{ primo}$$

DIM

$\text{MCD}(a, p^r) = 1$ per $a = 1, \dots, p^r$ a meno che $p | a$

Il numero di multipli di p im $\{0, \dots, p^r-1\}$ è p^{r-1} (se $p | a$)



ESEMPI

i) $p = 3, r = 2$

$$\{0, \dots, p^{r-1}\} = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$$

elem. multipli di p : $p^{r-1} = 3^{2-1} = 3$ (e sono 0, 3, 6)

$$\# \text{ unità}: p^r(1 - \frac{1}{p}) = p^r - p^{r-1} = 3^2 - 3 = 5$$

ii) $p = 2, r = 3$

$$\{0, \dots, p^{r-1}\} = \{0, 1, 2, 3, 4, 5, 6, 7\}$$

elem. multipli di p : $p^{r-1} = 2^{3-1} = 4$ (e sono 0, 2, 4, 6)

$$\# \text{ unità}: p^r(1 - \frac{1}{p}) = p^r - p^{r-1} = 2^3 - 4 = 4$$

LEMMA

Siamo A e B insiemi finiti con la stessa cardinalità.

Allora, le seguenti affermazioni sono equivalenti:

- $f: A \rightarrow B$ è iniettiva
- $f: A \rightarrow B$ è suriettiva

(cioè $f: A \rightarrow B$ imj $\Rightarrow f: A \rightarrow B$ surj

$f: A \rightarrow B$ surj $\Rightarrow f: A \rightarrow B$ imj)

DIM

$$f: A \rightarrow B \text{ imj} \Rightarrow |f(A)| = |A| \Rightarrow |f(A)| = |A| = |B| \Rightarrow f \text{ surj}$$

$$f: A \rightarrow B \text{ non imj} \Rightarrow |f(A)| < |A| = |B| \Rightarrow f \text{ non surj}$$

□

Supponiamo $\text{MCD}(m, n) = 1$ dove $m, n \geq 1$.

Allora, dati $a, b \in \mathbb{Z}$ $\exists c \in \mathbb{Z}$ t.c.:

- $c \equiv a \pmod{m}$
- $c \equiv b \pmod{n}$

DIM

Per il th di Bezout $\exists u, v$ t.c. $mu + nv = \text{MCD}(m, n) = 1$

Sia $c = anv + bmu$.

Allora:

- $c = a(\underbrace{1-mu}_{nv}) + bmu = a + \cancel{mu}(b-a) \equiv a \pmod{m}$
- $c = anv + b(\underbrace{1-nv}_{mu}) = \cancel{nv}(a-b) + b \equiv b \pmod{n}$

□

CONSEQUENZA

Supponiamo che m, n siano interi > 1 t.c. $\text{MCD}(m, n) = 1$.

Allora, la mappa $f: \mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$, $f([x]_{mn}) = ([x]_m, [x]_n)$ è una biiezione.

DIM

La suriettività di f segue da $c \equiv a \pmod{m}, c \equiv b \pmod{n}$

$|\mathbb{Z}_{mn}| = |\mathbb{Z}_m| |\mathbb{Z}_n| = mn \Rightarrow f \text{ imj} \Rightarrow f \text{ è una biiezione}$

□

PROPOSIZIONE

Supponiamo che m e n siano interi > 1 t.c. $\text{MCD}(m, n) = 1$

Siamo:

$A = \mathbb{Z}$ insieme delle unità in \mathbb{Z}_m

$B = \mathbb{Z}$ insieme delle unità in \mathbb{Z}_n

$C = \mathbb{Z}$ insieme delle unità in \mathbb{Z}_{mn}

Allora, la mappa $f: \mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$, $f([x]_{mn}) = ([x]_m, [x]_n)$

è una biiezione da C a $A \times B$ ($f: C \rightarrow A \times B$) -

In particolare $\phi(mn) = |C| = |A||B| = \phi(m)\phi(n)$

DIM

Per def. $f^{-1}(A \times B) = \{[x] \in \mathbb{Z}_{mn} : f(x) \in A \times B\}$

Poiché $f: \mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$ è una biiezione, f si restringa a una biiezione $f^{-1}(A \times B) \rightarrow A \times B$.

- $f^{-1}(A \times B) \subseteq C$

$$([\alpha]_m, [\beta]_n) \in A \times B$$

$$\Rightarrow \exists [c]_{mn} \in \mathbb{Z}_{mn} \text{ t.c. } f([c]) = ([\alpha]_m, [\beta]_n)$$

$$\exists [c']_{mn} \in \mathbb{Z}_{mn} \text{ t.c. } f([c']) = ([\alpha]_m^{-1}, [\beta]_n^{-1})$$

$$\Rightarrow f([c]_{mn} [c']_{mn}) = f(c) f(c') = ([\alpha]_m, [\beta]_n) ([\alpha]_m^{-1}, [\beta]_n^{-1}) = \\ = ([1]_m, [1]_n) = [1]_{mn}$$

- $C \subseteq f^{-1}(A \times B)$

Supponiamo che $[c]_{mn} \in \mathbb{Z}_{mn}$ sia un'unità.

$$\Rightarrow \text{MCD}(c, mn) = 1$$

per Bézout $\Rightarrow \exists \mu, \nu \in \mathbb{Z} \text{ t.c. } c\mu + (mn)\nu = 1$

$$\Rightarrow c\mu + m(n\nu) = 1 \Rightarrow \text{MCD}(c, m) = 1$$

$$c\mu + n(m\nu) = 1 \Rightarrow \text{MCD}(c, n) = 1$$

$$\Rightarrow [c]_m [\mu]_m = [1]_m$$

$$[c]_n [\mu]_n = [1]_n$$

$$\Rightarrow [c]_m \text{ è un'unità di } \mathbb{Z}_m \quad [c]_n \text{ è un'unità di } \mathbb{Z}_n$$

$$\Rightarrow f(c) = [c]_{mn} \in f^{-1}(A \times B)$$

□

ESEMPIO

$$\phi(36) = \phi(\underbrace{2^2 \cdot 3^2}) = \phi(2^2) \phi(3^2) =$$

FAZOLIET.
POTENZA
DI 36 $= 4(1 - \frac{1}{2}) 9(1 - \frac{1}{3}) = \\ = (4 - 2)(9 - 3) = 12$

PROPOSIZIONE (PRODOTTO DI EULEO)

Se n è un intero positivo, allora:

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right), p \text{ primo}$$

DIM

Sia $n = p_1^{r_1} \cdots p_k^{r_k}$ la fattorizz. prima di n .

$$\begin{aligned} \Rightarrow \phi(n) &= \phi(p_1^{r_1}) \cdots \phi(p_k^{r_k}) = \\ &= p_1^{r_1} \left(1 - \frac{1}{p_1}\right) \cdots p_k^{r_k} \left(1 - \frac{1}{p_k}\right) = \frac{n \prod_{j=1}^k p_j^{r_j}}{p_1^{r_1} \cdots p_k^{r_k}} \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right) \end{aligned}$$

□

TH (EULEO, GENERALIZZ. DEL PICCOLO TH DI FERMAT)

Siamo a e n interi positivi con $n > 1$

$$\text{MCD}(a, n) = 1 \Rightarrow a^{\phi(n)} \equiv 1 \pmod{n}$$

DIM

Se R è un anello comm. con id. \Rightarrow il prodotto di due unità di R è ancora un'unità di R
(Se x, y hanno un inverso molt., anche xy ha un inverso molt.).

Siamo $R = \mathbb{Z}/n\mathbb{Z}$, $S = \mathbb{Z}/n\mathbb{Z}$: l'insieme delle unità in R

$$\Rightarrow |S| = \phi(n), u = \prod_{s \in S} s \text{ è un'unità}$$

Sia $v \in S$.

Allora, la mappa $f: S \rightarrow R$, $f(s) = vs$ ha immagine contenuta in S perché $(vs)^{-1} = v^{-1}s^{-1}$.

Inoltre, poiché v è un'unità, f è iniettiva.

$$f(s) = f(s') \Rightarrow vs = vs' \Rightarrow s = s'$$

$|S| < \infty \Rightarrow f: S \rightarrow S$ è una biiezione

$$\Rightarrow u = \prod_{s \in S} s = \prod_{s \in S} f(s) = \prod_{s \in S} vs = v \prod_{s \in S} s = v^{\phi(n)}$$

$$\Rightarrow v^{\phi(n)} = 1$$

$\text{MCD}(\alpha, n) = 1 \Rightarrow [\alpha] \in R$ é um' unitá'

Ponendo $v = [\alpha]$ si ha $[\alpha]^{\phi(n)} = [1]$, cioè $\alpha^{\phi(n)} \equiv 1 \pmod{n}$

□

TH (GAUSS)

Sia n un intero positivo.

Allora $\sum_{d|n} \phi(d) = n$

ESEMPPIO

$$n = 20$$

$$\phi(20) = \phi(2^2 \cdot 5) = 4\left(1 - \frac{1}{2}\right)5\left(1 - \frac{1}{5}\right) = 8$$

Per il th di Gauss:

$$\begin{aligned} n = 20 &= \sum_{d|20} \phi(d) = \phi(1) + \phi(2) + \phi(4) + \phi(5) + \phi(10) + \phi(20) \\ &= 1 + 1 + 2 + 4 + 4 + 8 \\ &= 20 \quad \checkmark \end{aligned}$$

DEF (GRUPPO)

Un gruppo $(G, *)$ consiste di un insieme G con una mappa $*: G \times G \rightarrow G$ con le seguenti proprietà:

- ASSOCIAZIONE: $(a * b) * c = a * (b * c) \quad \forall a, b \in G$
- IDENITÀ: $\exists e \in G \text{ t.c. } e * a = a * e = a \quad \forall a \in G$
- INVERSO: $\forall a \in G \exists a^{-1} \in G \text{ t.c. } a * a^{-1} = a^{-1} * a = e$

□: cioè l'insieme G deve essere chiuso rispetto all'oper. $*$

DEF (GRUPPO ABELIANO)

Un gruppo abeliano è un gruppo $(G, *)$ t.c.

$a * b = b * a \quad \forall a, b \in G$ (cioè t.c. $*$ è commutativa)

[PER NOTAZIONE ED ESEMPI VEDI LEZIONE 8-9]

DEF (SOTTOGRUPPO)

Un sottoinsieme H di un gruppo G è un sottogruppo \Leftrightarrow :

- H contiene l'elemento identità $e \in G$
- $a \in H \Rightarrow a^{-1} \in H$
- $a, b \in H \Rightarrow a * b \in H$

(cioè H è un sottoinsieme di G chiuso rispetto all'operazione $*$ di G)

[PER ESEMPI VEDI LEZIONE 8-9]

LEMMA

Sia G un gruppo.

Allora, un sottoinsieme non vuoto H di G è un sottogruppo

$$\Leftrightarrow a, b \in H \Rightarrow ab^{-1} \in H$$

DM

$$H \neq \emptyset \Rightarrow \exists a \in H \Rightarrow aa^{-1} = e \in H$$

$$b \in H \Rightarrow eb^{-1} = b^{-1} \in H$$

$$\Rightarrow a, b \in H \Rightarrow \underbrace{a(b^{-1})^{-1}}_{=b} = ab \in H$$

perché $bb^{-1} = b^{-1}b = e$ poiché b^{-1} è l'inverso di b
 $\Rightarrow b$ è l'inverso di b^{-1} , cioè $b = (b^{-1})^{-1}$

Viceversa:

$$H \text{ sottogruppo di } G \Rightarrow e \in H \Rightarrow H \neq \emptyset$$

Poiché H è chiuso rispetto alla moltip. e agli inversi:

$$a, b \in H \Rightarrow ab^{-1} \in H$$

□

LEMMA

Sia H un sottogruppo di $(G, *)$.

Allora H è un gruppo rispetto alla restruzione di $*$ ad H .

DM

Dobbiamo dim. che $(H, *_H)$ è un gruppo dove $*_H$ è definita come $*_H: H \times H \rightarrow H$.

- H sottogruppo di $(G, *) \Rightarrow *_H$ è associativa
- H sottogruppo di $(G, *) \stackrel{\text{per def.}}{\Rightarrow} a \in H \Rightarrow a^{-1} \in H$
- $\exists e \in H$ t.c. $e = a *_H a^{-1} \in H \quad \forall a \in H$

□

LEMMA

Siamo H e K sottogruppi di G .

Allora $H \cap K$ è un sottogruppo di G .

DIM

H sottogruppo di $G \Rightarrow e \in H$

K sottogruppo di $G \Rightarrow e \in K$

$\Rightarrow e \in H \cap K \Rightarrow H \cap K \neq \emptyset$ ($\therefore H \cap K$ contiene l'identità e)

Siamo $x, y \in H \cap K$

$\Rightarrow x, y \in H, x, y \in K$

H sottogruppo di $G \Rightarrow H$ chiuso rispetto all'operazione su G

$\Rightarrow xy \in H$

K sottogruppo di $G \Rightarrow K$ chiuso rispetto all'operazione su G

$\Rightarrow xy \in K$

$\Rightarrow xy \in H \cap K$ ($\therefore H \cap K$ è chiuso rispetto all'op. su G)

Sia $z \in H \cap K$.

$\Rightarrow z \in H, z \in K$

H sottogruppo di $G \Rightarrow H$ chiuso rispetto agli inversi

$\Rightarrow z^{-1} \in H$

K sottogruppo di $G \Rightarrow K$ chiuso rispetto agli inversi

$\Rightarrow z^{-1} \in K$

$\Rightarrow z^{-1} \in H \cap K$ ($\therefore H \cap K$ è chiuso rispetto agli inversi)

$\Rightarrow H \cap K$ è un sottogruppo di G

□

LEMMA

L'unione di due sottogruppi H e K di G è un sottogruppo
 $\Leftrightarrow H \subseteq K \circ K \subseteq H$

DIM

P: $H \cup K$ è un sottogruppo di G

Q: $H \subseteq K \circ K \subseteq H$

Allora:

- $Q \Rightarrow P$: $H \cup K = H \circ H \cup K = K$, quindi è un sottogruppo
- $P \Rightarrow Q$:

Consideriamo il contrapposito $\neg Q \Rightarrow \neg P$

Per def. $\neg Q \Rightarrow \exists h \in H, k \in K$ t.c. $h \notin K, k \notin H$

Supponiamo che $H \cup K$ sia un sottogruppo.

Allora $hk \in H \cup K$ e quindi $hk \in H \circ hk \in K$

$hk \in H \Rightarrow k = h^{-1}hk \in H$ $\frac{\downarrow}{\nmid}$

$hk \in K \Rightarrow h = hk(k^{-1}) \in K$ $\frac{\downarrow}{\nmid}$

$\therefore \neg Q \Rightarrow \neg P$

□

DEF (SOTTOGRUPPO $\langle S \rangle$ DI G GENERATO DA S)

Sia S un sottoinsieme di un gruppo G .

Allora, il sottogruppo $\langle S \rangle$ di G generato da S è

$\langle S \rangle = \bigcap_{S \subseteq H} H$, con H sottogruppo di G .

(cioè l'intersezione di tutti i sottogruppi H di G che contengono S)

LEMMA

$\langle S \rangle$ consiste di tutti i prodotti finiti di elem. $s_1 \dots s_r$ dove ogni $s_j \circ s_j^{-1} \in S$.

DIM

Sia H l'insieme di tutti i prodotti finiti $s_1 \dots s_r$ dove ogni $s_j \circ s_j^{-1} \in S$.

Per def., il prodotto vuoto è e, perciò $e \in H$.

$a, b \in H \Rightarrow ab$ è un prodotto finito di elementi di S e dei loro inversi, quindi $ab \in H$.

Allo stesso modo:

$$a = s_1 \dots s_r \in H \Rightarrow a^{-1} = s_r^{-1} \dots s_1^{-1} \in H$$

$\Rightarrow H$ sottogruppo di G che contiene $S \xrightarrow{\text{PER DEF.}} \langle S \rangle \subseteq H$

Viceversa, $H \subseteq S$ perché ogni sottogruppo K di G che contiene S deve contenere tutti i prodotti finiti degli elem. di S e degli inversi.

□

DEF (GRUPPO CIClico)

Un gruppo G è ciclico $\Leftrightarrow G = \langle g \rangle$ per qualche $g \in G$.

NOTA: G ciclico $\Rightarrow G$ abeliano

G non abeliano $\Rightarrow G$ non ciclico

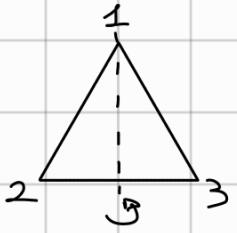
DEF (ORDINE DI UN GRUPPO)

Sia G un gruppo.

Se G è finito, allora $\text{ord}(G) = |G|$, altrimenti $\text{ord}(G) = \infty$

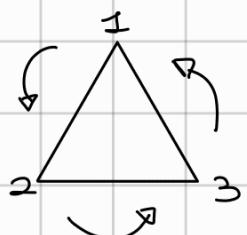
Se $g \in G$ allora $\text{ord}(g) = \text{ord}(\langle g \rangle)$.

ESEMPIO



$$\sigma: \{1, 2, 3\} \rightarrow \{1, 3, 2\}$$

$$\text{ord}(\sigma) = |\langle \sigma \rangle| = |\{\sigma, \sigma^2 = I\}| = 2$$



$$\rho: \{1, 2, 3\} \rightarrow \{3, 2, 1\}$$

$$\text{ord}(\rho) = |\langle \rho \rangle| = |\{\rho, \rho^2, \rho^3 = I\}| = 3$$

LEMMA

Sia H un sottoinsieme finito non vuoto di un gruppo G , dove H è chiuso rispetto alla moltiplicazione.
Allora, H è un sottogruppo di G .

DIM

Le ipotesi su G e H implicano che:

$$\{h, h^2, h^3, \dots\} \subseteq H \text{ è finito}$$

In particolare $\exists r, s \in \mathbb{Z}, r, s > 0, r \neq s$ t.c. $h^r = h^s$

Scambiando r e s se necessario, assumiamo $s > r$.

$$\Rightarrow h^r = h^r h^{s-r} \Rightarrow h^{s-r} = e$$

$$s-r=1 \Rightarrow h=e, \text{ altrimenti } s-r > 1$$

$$\Rightarrow hh^{s-r-1}=e \Rightarrow h^{-1} \in H$$

□

DEF (CENTRALIZZANTE)

Sia G un gruppo e $x \in G$.

Allora, $C(x) = \{g \in G : gx = x\}$ è un sottogruppo di G

Chiamato il centralizzante di x .

DIM (che $C(x)$ è un sottogruppo)

- $ex = xe \Rightarrow e \in C(x)$

- $a x = x a, b x = x b \Rightarrow abx = axb = xab \Rightarrow ab \in C(x)$

- $a x = x a \Rightarrow a^{-1} a x = a^{-1} x a \Rightarrow x = a^{-1} x a$

$$\Rightarrow x a^{-1} = a^{-1} x a a^{-1} \Rightarrow x a^{-1} = x a^{-1} \Rightarrow a^{-1} \in C(x)$$

PROPOSIZIONE

Siamo H e K dei gruppi.

Allora, $H \times K$ è un gruppo rispetto all'operazione bimaria $(h_1, k_1) * (h_2, k_2) = (h_1 h_2, k_1 k_2)$ con elemento identità $e = (e_H, e_K)$.

Se H e K sono gruppi finiti, allora $\text{ord}(H \times K) = \text{ord}(H) \cdot \text{ord}(K)$

Altrimenti $H \times K$ ha ordine infinito.

DIM

- H, K gruppi $\Rightarrow H \times K$ gruppo rispetto a *

$$\begin{aligned} i) ((h_1, k_1)(h_2, k_2))(h_3, k_3) &= (h_1 h_2, k_1 k_2)(h_3, k_3) = \\ &= (h_1 h_2 h_3, k_1 k_2 k_3) \end{aligned}$$

$$\begin{aligned} (h_1, k_1)((h_2, k_2)(h_3, k_3)) &= (h_1, k_1)(h_2 h_3, k_2 k_3) = \\ &= (h_1 h_2 h_3, k_1 k_2 k_3) \end{aligned} \quad \checkmark$$

$$ii) (e_H, e_K)(h, k) = (h, k)(e_H, e_K) = (h, k) \quad \checkmark$$

$$iii) (h, k)(h, k)^{-1} = (h, k)^{-1}(h, k) = (e_H, e_K) \quad \checkmark$$

- H, K gruppi finiti $\Rightarrow \text{ord}(H \times K) = \text{ord}(H) \times \text{ord}(K)$

$$H \times K = \{(h, k) : h \in H, k \in K\}$$

Si hanno $\binom{\text{ord}(H)}{1} = \text{ord}(H)$ scelte per h e $\binom{\text{ord}(K)}{1} = \text{ord}(K)$ scelte per k .

Le scelte di h e k sono indipendenti, quindi possiamo moltiplicare: $\text{ord}(H) \cdot \text{ord}(K)$

$$\Rightarrow \text{ord}(H \times K) = \text{ord}(H) \cdot \text{ord}(K)$$

□

DEF (ISOMORFISMO)

Siamo G e H gruppi.

Allora, $f: G \rightarrow H$ è un isomorfismo se e solo se:

- f è biettiva
- $f(g_1 g_2) = f(g_1) f(g_2) \quad \forall g_1, g_2 \in G$

Diciamo che una coppia di gruppi G e H sono isomorfi se e solo se esiste un isomorfismo $f: G \rightarrow H$ (\Rightarrow scriviamo $G \cong H$).

CONTROESEMPIO

$\mathbb{Z}_2 \times \mathbb{Z}_2 \not\cong \mathbb{Z}_4$ perché:

$f: \mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$ è una biezione se $\text{MCD}(m,n)=1$
ma $\text{MCD}(2,2)=2 \Rightarrow f$ non è una biezione
 $\Rightarrow f$ non è un isomorfismo

Alternativamente:

$$([\alpha]_2, [\beta]_2) \in \mathbb{Z}_2 \times \mathbb{Z}_2$$

$$\Rightarrow ([\alpha]_2, [\beta]_2) + ([\alpha]_2, [\beta]_2) = ([2\alpha]_2, [2\beta]_2) = ([0]_2, [0]_2)$$

$$\Rightarrow \text{ord}([\alpha]_2, [\beta]_2) \leq 2$$

mentre

$$[\alpha]_4 \in \mathbb{Z}_4$$

$$\Rightarrow [\alpha]_4 + [\alpha]_4 + [\alpha]_4 + [\alpha]_4 = [4\alpha]_4 = [0]_4$$

$$\Rightarrow \text{ord}([\alpha]_4) = 4$$

Poiché \mathbb{Z}_4 ha un elemento di ordine 4 e $\mathbb{Z}_2 \times \mathbb{Z}_2$ no,
i due gruppi non sono isomorfi.

ESEMPIO

$\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$ perché:

- $\text{MCD}(2,3) = 1 \Rightarrow f: \mathbb{Z}_6 \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_3$ è una biiezione ✓
 - $f([x]_6) = ([x]_2, [x]_3)$
 - $f([y]_6) = ([y]_2, [y]_3)$
- $\Rightarrow f([xy]_6) = f([x]_6)f([y]_6)_6$ ✓

Alternativamente:

$$([\alpha]_2, [\beta]_3) \in \mathbb{Z}_2 \times \mathbb{Z}_3$$

$$\Rightarrow ([\alpha]_2, [\beta]_3) + ([\alpha]_2, [\beta]_3) = ([2\alpha]_2, [2\beta]_3) \neq ([0]_2, [0]_3)$$

$$([\alpha]_2, [\beta]_3) + ([\alpha]_2, [\beta]_3) = ([3\alpha]_2, [3\beta]_3) \neq ([0]_2, [0]_3)$$

$$([\alpha]_2, [\beta]_3) + ([\alpha]_2, [\beta]_3) = ([4\alpha]_2, [4\beta]_3) \neq ([0]_2, [0]_3)$$

$$([\alpha]_2, [\beta]_3) + ([\alpha]_2, [\beta]_3) = ([5\alpha]_2, [5\beta]_3) \neq ([0]_2, [0]_3)$$

$$([\alpha]_2, [\beta]_3) + ([\alpha]_2, [\beta]_3) = ([6\alpha]_2, [6\beta]_3) = ([0]_2, [0]_3)$$

$$\Rightarrow \text{ord}([\alpha]_2, [\beta]_3) \leq 6$$

$$[\alpha]_6 \in \mathbb{Z}_6$$

$$\Rightarrow [\alpha]_6 + [\alpha]_6 + [\alpha]_6 + [\alpha]_6 + [\alpha]_6 + [\alpha]_6 = [0]_6$$

$$\Rightarrow \text{ord}([\alpha]_6) = 6$$

PROPOSIZIONE (FOGLIA DESSOLE DEL TH CHINESE DEL RESTO)

Siamo n_1, \dots, n_k interi > 1 t.c. $\text{MCD}(n_i, n_j) = 1$ se $i \neq j$.

Allora $\mathbb{Z}_{n_1 \dots n_k} \cong \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$

DIM

$\text{MCD}(n_i, n_j) = 1$ se $i \neq j \Rightarrow n_1, \dots, n_k$ non hanno fattori primi comuni

$$\Rightarrow \text{MCD}(n_1 \dots n_j, n_{j+1} \dots n_k) = 1$$

$$\Rightarrow \mathbb{Z}_{n_1 \dots n_k} \cong \mathbb{Z}_{n_1} \times (\mathbb{Z}_{n_2} \times \dots \times \mathbb{Z}_{n_k}) \cong \dots \cong \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$$

□

ESEMPIO

$$\mathbb{Z}_{4 \cdot 9 \cdot 5 \cdot 7} = \mathbb{Z}_4 \times \mathbb{Z}_{9 \cdot 5 \cdot 7} = \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_{5 \cdot 7} = \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \cdot \mathbb{Z}_7$$

TH DEL FATTORE INVARIANTE (GAUSS, ...)

finito.

Sia G un gruppo abeliano non banale (cioè $G \neq \{e\}$)
Allora c'è un unico insieme di divisori d_1, \dots, d_r di $|G|$ t.c:

- $|G| = d_1 \cdots d_r$ dove $d_j > 1 \forall j$
- $G \cong \mathbb{Z}_{d_1} \oplus \mathbb{Z}_{d_2} \oplus \cdots \oplus \mathbb{Z}_{d_r}$
- $d_r | d_{r-1}, \dots, d_1 | d$

La lista (d_1, \dots, d_r) viene detta **LISTA DEI FATTORE INVARIANTI** di G
una coppia di gruppi abeliani G e H sono isomorfi se e solo se hanno gli stessi fattori invarianti.

ESEMPIO

$$|G| = 36$$

LISTA FATTORE INVARIANTI:

- (36)
- $(18, 2)$
- $(12, 3)$
- $(6, 6)$

=> Esistono 4 tipi di gruppi abeliani con $|G| = 36$:

$$\underbrace{\mathbb{Z}_{36}}, \underbrace{\mathbb{Z}_{18} \times \mathbb{Z}_2}, \underbrace{\mathbb{Z}_{12} \times \mathbb{Z}_3}, \underbrace{\mathbb{Z}_6 \times \mathbb{Z}_6}$$

$$\downarrow \quad \quad \quad \downarrow \quad \quad \quad \downarrow \quad \quad \quad \downarrow$$

$$\text{ord} = 36 \quad \text{ord} \leq 18 \quad \text{ord} \leq 12 \quad \text{ord} \leq 6 \quad => \text{i 4 gruppi man}$$

sono isomorfi
tra loro

Siamo $a \neq b$ due fattori primi distinti di n .

• $n = a^2 b^2$

\Rightarrow la lista dei fattori invarianti di un gruppo abeliano di ordine n è:

$$(a^2 b^2), (ab^2, a), (a^2 b, b), (ab, ab)$$

• $n = a^2 b^3$

$$\Rightarrow (a^2 b^3), (ab^3, a), (a^2 b^2, b), (ab^2, ab), (a^2 b, b, b), (ab, ab, b)$$

PROPOSIZIONE

Sia $n > 1$ un intero positivo privo di quadrati.

Allora c'è esattamente un gruppo abeliano di ordine n .

DIM

n privo di quadrati \Rightarrow ogni fattore primo di n compare con la potenza 1

$\Rightarrow (n)$ è l'unico possibile fattore invariante

□

Più in generale, per calcolare il num. di possibili gruppi abeliani di ordine n , ricordiamo che una partizione di n è una somma della forma:

$$n = a_1 + \dots + a_m, a_i \text{ intero positivo}$$

Due partizioni sono equivalenti se sono uguali a meno di riordinamento.

Es

Le partizioni di 4 sono:

$$4, 3+1, 2+2, 2+1+1, 1+1+1+1$$

Se l è un intero positivo, sia $\pi(l)$ il num. di partizioni equivalenti di l .

Il seguente th è una conseguenza del th del fattore invarianto.

TH

Sia $n > 1$ un intero con fattori p_1, \dots, p_r . Poi $n = p_1^{k_1} \cdots p_r^{k_r}$. Allora, il num. di gruppi abeliani di ordine n è $\pi(k_1) \cdots \pi(k_r)$.

Sia H un sottogruppo di G .

Sia \sim la relazione su G definita da $a \sim b \Leftrightarrow a^{-1}b \in H$.

Ricordiamo che se G è un gruppo, allora:

$$(xy)^{-1} = y^{-1}x^{-1} \text{ e } (x^{-1})^{-1} = x$$

LEMMA

$a \sim b \Leftrightarrow a^{-1}b \in H$ è una relazione di equivalenza.

DIM

- $a \sim a : a^{-1}a \in H$
- $a \sim b \Rightarrow b \sim a :$
 $a \sim b \Leftrightarrow a^{-1}b \in H \Rightarrow (a^{-1}b)^{-1} \in H \Rightarrow b^{-1}a \in H \Rightarrow b \sim a$
- $a \sim b, b \sim c \Rightarrow a \sim c :$
 $a \sim b \Rightarrow a^{-1}b \in H, b \sim c \Rightarrow b^{-1}c \in H$
 $\Rightarrow (a^{-1}b)(b^{-1}c) = a^{-1}c \in H \Rightarrow a \sim c$

□

DEF (COSET, CLASSE LATERALE (sx))

Sia H un sottogruppo di G e $a \in G$.

Allora, $aH = \{ah : h \in H\}$ è chiamato il coset (classe laterale) sinistro di a .

PROPOSIZIONE

Siamo H un sottogruppo di G e $a, b \in G$.

Allora, $a \sim b \Leftrightarrow b \in aH$

DIM

- $a \sim b \Rightarrow a^{-1}b = h \in H \Rightarrow b = ah \in aH$
- $b \in aH \Rightarrow b = ah$ per un qualche $h \in H$
 $\Rightarrow a^{-1}b = h \in H \Rightarrow a \sim b$

□

DEF

Sia H un sottogruppo di G .

Allora, l'indice $[G : H]$ è la cardinalità di G/H .

TH (LAGRANGE)

Sia H un sottogruppo di un gruppo finito G .

Allora $|G| = \underbrace{[G : H]}_{\parallel} |H|$

(N.B.: non è vero il viceversa, in particolare, per def. un gruppo finito G ha un elem. di ordine $|G| \Leftrightarrow G$ ciclico)

Per la proposizione precedente:

$$[a] = aH \Rightarrow |[a]| = |aH| = |H| \leq |G| < \infty$$

\sim rel. di equiv. $\Rightarrow G = \bigcup_i [a_i]$ (cioè G è un'unione disgiunta di classi di equiv.)
 $\Rightarrow |G| = \sum_i |[a_i]| = [G : H] |H|$

perché ci sono $[G : H]$ cosets

□

COROLLAIO

Sia g un elemento di un gruppo finito G .

Allora $\text{ord}(g) | \text{ord}(G) = |G|$

DIM

$\text{ord}(g) = |\langle g \rangle|$, $H = \langle g \rangle$ è un sottogruppo di G .
 $\Rightarrow |G| = [G : H] |H| \Rightarrow \text{ord}(g) | \text{ord}(G)$

□

ESEMPIO

$$G = \mathbb{Z}_2 \times \mathbb{Z}_2$$

$\text{ord}(G) \leq 2$, infatti:

$$\text{ord}(0,0) = 1$$

$$\text{ord}(1,0) = 2 \quad \text{perché } \langle(1,0)\rangle = \{(1,0), (0,0)\}$$

$$\text{ord}(0,1) = 2 \quad " \quad \langle(0,1)\rangle = \{(0,1), (0,0)\}$$

$$\text{ord}(1,1) = 2 \quad " \quad \langle(1,1)\rangle = \{(1,1), (0,0)\}$$

TEOREMA

Sia p un num. primo e G un gruppo di ordine p .

Allora G è isomorfo a $(\mathbb{Z}_p, +)$.

DIM

Sia $g \in G - \{e\}$.

Per il th di Lagrange, $\text{ord}(g) | \text{ord}(G) = p$

Allora, poiché p è primo, $\text{ord}(g) = 1$ oppure $\text{ord}(g) = p$.

Ma $\text{ord}(g) \neq 1$ perché $g \neq e$.

$\Rightarrow \langle g \rangle$ (sottogruppo di G generato da g) ha ordine p .

$$\Rightarrow \langle g \rangle = G$$

Come tale, $f(r) = g^r$ definisce un isomorfismo da $(\mathbb{Z}_p, +)$ a G .

□

PICCOLO TH DI FERMAT

Sia p un numero primo e n un intero.

Allora $p \mid n^p - n$ (cioè $n^p - n \equiv 0 \pmod{p}$).

DIM

Se p è un numero primo allora $U(p) = \mathbb{Z}_p - \{0\}$ è il gruppo di unità in \mathbb{Z}_p rispetto alla moltiplicazione.

$$|U(p)| = p - 1$$

$$[n] \in U(p) \Rightarrow \text{ord}([n]) \mid \text{ord}(U(p)) = p - 1 \quad \text{PER LAGRANGE}$$

$$[n] = 0 \Rightarrow n^p - n \equiv 0 \pmod{p}$$

$$\begin{aligned}[n] \neq 0 &\Rightarrow n^{p-1} \equiv 1 \pmod{p} \\ &\Rightarrow n \cdot n^{p-1} \equiv n \pmod{p} \\ &\Rightarrow n^p - n \equiv 0 \pmod{p}\end{aligned}$$

□

TH DI EULER

Siamo a e n interi positivi con $n > 1$.

Se $\text{MCD}(a, n) = 1$ allora $a^{\phi(n)} \equiv 1 \pmod{n}$.

DIM

Sia $U(n)$ il gruppo di unità in \mathbb{Z}_n rispetto alla moltiplicazione.

$$|U(n)| = \phi(n)$$

$$\text{MCD}(a, n) = 1 \Rightarrow [a] \in U(n) \Rightarrow a^{\phi(n)} \equiv 1 \pmod{n}$$

□

DEF (ELEMENTI CONIUGATI)

Se G è un gruppo, $x, y \in G$ sono coniugati se $\exists g \in G$
t.c. $x = gyg^{-1}$ -

In questo caso scriviamo $x \sim y$.

PROPOSIZIONE

\sim è una relazione di equivalenza

DIM

- $x \sim x : x = exe^{-1}$
- $x \sim y \Rightarrow y \sim x : x = gyg^{-1} \Rightarrow y = g^{-1}xg$
- $x \sim y, y \sim z \Rightarrow x \sim z : x \sim y \Rightarrow x = gyg^{-1}, y \sim z \Rightarrow y = hzh^{-1}$

$$\text{Allora } x = ghzg^{-1}g^{-1} = (gh)z(gh)^{-1} \\ \Rightarrow x \sim z$$

□

DEF (CLASSE DI CONIUGIO)

$C(x) =$ classe di equivalenza di $x \in G$ rispetto a \sim .

Se G è finito, $|C(x)| = |G/C(x)| = [G:C(x)]$ -

Per il th di Lagrange, $|C(x)| \mid |G|$ -

DEF (CENTRO DI UN GRUPPO)

$$Z(G) = \{x \in G : gx = xg \ \forall g \in G\}$$

$Z(G)$ è un sottogruppo di G .

DIM

- $eg = ge \ \forall g \in G \Rightarrow e \in Z(G)$

- $x, y \in Z(G)$

\uparrow PERCHÉ $y \in Z(G)$

PROPRIETÀ
ASSOCIAZIONE

$$(xy)g = x(yg) = x(gy) = xg(y) = (gx)y = g(xy) \quad \forall g \in G$$

- $x \in Z(G)$

$$x^{-1}g = x^{-1}(gx)x^{-1} = x^{-1}(xg)x^{-1} = egx^{-1} = g x^{-1} \quad \forall g \in G$$

□

[vedi esempio p.11 lezione 8-9]

TH (FORMULA DELLE CLASSI DI CONIUGIO)

Sia G un gruppo finito.

Allora, $|G| = |Z(G)| + \sum_{|\langle x_j \rangle| > 1} [G : C(x_j)]$

FORMULA DELLE
CLASSI DI CONIUGIO
DI G

Un'applicazione di questa formula è la seguente:

Supponiamo di sapere solo che G è un gruppo con $n > 1$ classi di coniugio.

Consideriamo tutte le possibili soluzioni dell'eq.:

$$1 = \sum_{j=1}^n \frac{1}{a_j}, \quad a_j \in \mathbb{Z}$$

Il valore più grande di a_j costituisce un limite superiore all'ordine di G .

PROPOSIZIONE

Sia p un num. primo e G un gruppo di ordine $p^r > 1$. Allora $Z(G) \neq \{e\}$.

DIM

$$r=1 \Rightarrow G \cong \mathbb{Z}/p, Z(G) = G$$

Supponiamo quindi $r > 1$, $Z(G) = \{e\}$

Sia $g \in G - Z(G)$.

$$\text{Allora } \underbrace{C_G(g)}_{\neq 1} \mid \underbrace{|G|}_{= p^r}.$$

$$\Rightarrow |C_G(g)| = p^j \text{ per qualche } j > 0$$

$$g \in G - Z(G) \Rightarrow p^r = |G| = |Z(G)| + |C_G(g_1)| + \dots + |C_G(g_r)| = 1 + pk$$

per qualche intero k perché ogni
 $|C_G(g_i)| > 1$ è una potenza di p

$$\text{Ma } p^r = 1 + kp \Rightarrow kp = p^r - 1 = (p-1)(1+p+\dots+p^{r-1}) \text{ e quindi}$$

$$p \mid kp \Rightarrow p \mid (p-1)(1+p+\dots+p^{r-1}) \Rightarrow (p \mid p-1 \circ p \mid 1+p+\dots+p^{r-1}) \Rightarrow p \mid \pm 1$$

$$\Rightarrow |Z(G)| \neq 1$$

*

□

DEF (OMOOMORFISMO DI GRUPPI)

Siamo G e H gruppi.

Allora, una mappa $f: G \rightarrow H$ è un omomorfismo di gruppi $\Leftrightarrow f(g_1 g_2) = f(g_1) f(g_2) \quad \forall g_1, g_2 \in G$

(simile a una mappa lineare ma senza molt. scalare)

N.B.: un isomorfismo è un omomorfismo biettivo

PROPOSIZIONE

Se $f: G \rightarrow H$ è un omomorfismo di gruppi, allora $f(e_G) = e_H$ e $f(g^{-1}) = f(g)^{-1}$

DIM

- $e_G = e_G e_G \Rightarrow f(e_G) = f(e_G) f(e_G)$ PER LA DEF. DI OMOMORFISMO
 $\Rightarrow \underbrace{f(e_G) f(e_G)^{-1}}_{= e_H} = f(e_G) f(e_G) f(e_G)^{-1}$
 $\Rightarrow e_H = f(e_G)$
- Sia $g \in G$.
 $e_H = f(e_G) = f(gg^{-1}) = f(g) f(g^{-1})$

□

PROPOSIZIONE

Sia $f: G \rightarrow H$ un omomorfismo di gruppi -

Allora:

- $\text{Ker}(f) = \{g \in G : f(g) = e_H\}$ è un sottogruppo di G
- $\text{Im}(f) = \{f(g) : g \in G\}$ è un sottogruppo di H

DIM

Ricordiamo che un sottoinsieme non vuoto H di un gruppo G è un sottogruppo $\Leftrightarrow a, b \in H \Rightarrow a^{-1}b \in H$.

- $f(e_G) = e_H \Rightarrow e_G \in \text{Ker}(f)$
 $a, b \in \text{Ker}(f) \Rightarrow f(a^{-1}b) = f(a^{-1})f(b) = f(a)^{-1}f(b) =$
 $= e_H e_H = e_H$
 $\Rightarrow a^{-1}b \in \text{Ker}(f)$

- $f(e_G) = e_H \in \text{Im}(f)$

$$\begin{aligned} a &= f(\alpha), b = f(\beta) \in \text{Im}(f) \Rightarrow a^{-1}b = f(\alpha)^{-1}f(\beta) = \\ &= f(\alpha^{-1})f(\beta) = \\ &= f(\alpha^{-1}\beta) \\ \Rightarrow a^{-1}b &\in \text{Im}(f) \end{aligned}$$

□

Tutto ciò si poteva dimostrare anche tramite la def. di sottogruppo:

- i) • $f(e_G) = e_H \Rightarrow e_G \in \text{Ker}(f)$
 - $a, b \in \text{Ker}(f) \Rightarrow f(ab) = \underbrace{f(a)}_{e_H} \underbrace{f(b)}_{e_H} \text{ per la def. di } \text{Ker}(f)$
 $\Rightarrow f(ab) = e_H \Rightarrow ab \in \text{Ker}(f)$
 - $a \in \text{Ker}(f) \Rightarrow f(a^{-1}) = f(a)^{-1} = (e_H)^{-1} = e_H$
 $\Rightarrow a^{-1} \in \text{Ker}(f)$
- ii) • $f(e_G) = e_H \in \text{Im}(f)$
 - $a = f(\alpha), b = f(\beta) \in \text{Im}(f) \Rightarrow ab = f(\alpha)f(\beta) = f(\alpha\beta)$
 $\Rightarrow ab \in \text{Im}(f)$
 - $a = f(\alpha) \in \text{Im}(f) \Rightarrow a^{-1} = f(\alpha^{-1}) = f(\alpha)^{-1}$
 $\Rightarrow a^{-1} \in \text{Im}(f)$

□

DEF (SOTTOGRUPPO NORTELE)

Sia H un sottogruppo di G .

Allora, H è un sottogruppo normale di $G \Leftrightarrow gHg^{-1} = H \quad \forall g \in G$

In questo caso scriviamo $H \triangleleft G$.

NOTE:

- i) $H \triangleleft G \Rightarrow G/H$ è un gruppo con il seguente prodotto:
 $(aH)(bH) = a(bHb^{-1})(bH) = (abH)(b^{-1}bH) = (abH)H = (ab)H$
 G gruppo $\Rightarrow (aH)(bH) = (ab)H$ associativa
 $eH = H$ identità
 $(aH)(a^{-1}H) = H$
- ii) G gruppo abeliano $\Rightarrow H$ sottogruppo di G è normale

TH

Sia H un sottogruppo di G .

Allora, $(aH)(bH) = (ab)H$ definisce una struttura di gruppo su $G/H \Leftrightarrow H$ è un sottogruppo normale di G .

DIM

H sottogruppo normale di $G \Rightarrow G/H$ è un gruppo con l'operazione di prodotto indicata sopra.

$$\Rightarrow H = (aa^{-1}H) = (aH)(a^{-1}H) \Rightarrow H = aHa^{-1}$$

□

LEMMA

Sia $f: G \rightarrow H$ un omomorfismo di gruppi.

Allora, $\ker(f)$ è un sottogruppo normale di G .

DIM

Siamo $k \in \ker(f)$, $g \in G$.

$$\begin{aligned} \text{Allora, } f(gkg^{-1}) &= f(g)f(k)f(g^{-1}) = f(g)e_Hf(g^{-1}) = f(gg^{-1}) \\ &= f(e_G) = e_H \end{aligned}$$

$$\Rightarrow gkg^{-1} \in \ker(f)$$

□

LEMMA

Sia $f: G \rightarrow H$ un omomorfismo di gruppi e $K = \ker(f)$.

Allora, G/K è isomorfo a $\text{Im}(f)$.

DIM

Siamo $g \in G$, $k \in K$.

$$\text{Allora, } f(gk) = f(g)f(k) = f(g)$$

$F: G/K \rightarrow H$, $F(gk) = f(g)$ è ben definita e $\text{Im}(F) = \text{Im}(f)$.

Inoltre $F(gK) = F(gK') \Leftrightarrow f(g) = f(g')$ e

$$f(g) = f(g') \Rightarrow e_H = f(g)^{-1}f(g') = f(g^{-1}g') \Rightarrow g^{-1}g' \in K \Rightarrow gk = g'k$$

$\Rightarrow F: G/K \rightarrow \text{Im}(f)$ è una bijezione.

Poiché K è un sottogruppo normale di G :

$F((gk)(gk')) = F(gg'k) = f(gg') = f(g)f(g') = F(gk)F(g'k)$
 $\therefore F$ è un omomorfismo.

□

Proposizione

Siamo A un gruppo abeliano finito e p un fattore primo di $|A|$.

Allora, A ha un elemento di ordine p .

DIM

$P(q)$: $|A| = pq$, $q \geq 1 \Rightarrow A$ contiene un elem. di ordine p

• $P(1)$: $|A| = p \Rightarrow A \cong \mathbb{Z}/p$, che è ciclico di ordine p

Supponiamo $P(1), \dots, P(q)$ vere.

• $P(q+1)$:

Sia $\alpha \in A$ un elemento di ordine $d > 1$.

Se p è un fattore primo di d , allora $\alpha^{d/p}$ è un elemento di ordine p .

Supponiamo quindi che p non sia un fattore primo di d .

Per il th di Lagrange, $d | p(q+1)$ e quindi $d | (q+1)$.

Sia $C = \langle \alpha \rangle$ e $q' = (q+1)/d$.

Poiché A è un gruppo abeliano di ordine $p(q+1)$,

A/C è un gruppo abeliano di ordine pq' dove $q' < q+1$.

Dunque, per l'ip. induttiva, A/C ha un elemento (diverso dall'identità) y di ordine p .

Sia $f: A \rightarrow A/C$ l'omomorfismo quoziente.

f suriettiva $\Rightarrow \exists x \in A$ t.c. $f(x) = y$.

Sia $v > 0$ l'ordine di x e scriviamo $v = pu + r$ dove $0 \leq r < p$.

Allora, $f(e) = f(x^v) = f(x)^v = y^v = y^{pq+r} = y^r$ è l'elemento identità di A/C .

Dunque $r=0$ perché x ha ordine p .

Pertanto $p|x$ e quindi $x^{v/p} \in A$ è un elemento di ordine p .

□

NOTA: Infatti, per il th di Cauchy per gruppi finiti, se p è un fattore primo di $|G|$ allora G contiene un elemento di ordine p .

I th di Sylow affermano che p^n è la massima potenza di p che divide $|G|$, dunque $|G|$ ha un sottogruppo di ordine p^n .

DEF (OMOOMORFISMO DI ANELLI COMMUTATIVI CON IDENTITÀ)

Un omoomorfismo di anelli commutativi con identità è una mappa $f: R \rightarrow S$ che conserva tutte le strutture imerenti a tale anello.

In altre parole, $f: R \rightarrow S$ è un omoom. \Leftrightarrow :

- $f(x+y) = f(x) + f(y)$
- $f(xy) = f(x)f(y)$
- $f(1_R) = 1_S$

TH CHINESE DEL RESTO

Sia $\{n_1, \dots, n_k\}$ una collezione di interi > 1 e coprimi a coppie.

Allora:

$\Phi: \mathbb{Z}_{n_1, \dots, n_k} \rightarrow \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$, $\Phi([x]_{n_1, \dots, n_k}) = ([x]_{n_1}, \dots, [x]_{n_k})$
è un isomorfismo di anelli commutativi con identità.

DEF (CAMPO)

Sia R un anello commutativo con identità.

Allora, R è un campo se ogni elemento diverso da 0 di R ha un inverso moltiplicativo.

ESEMPIO

$\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$ (p primo) sono campi.

Se $n = ab$, $a, b > 1$ (n composto), \mathbb{Z}_n non è un campo perché $[a][b] = [ab] = 0$

$$\underline{\text{Es.}} \quad [2][3] = [6] = 0$$

in \mathbb{Z}_6

ESEMPIO

Se R è un dominio di integrità e $|R| < \infty$

$\Rightarrow R$ è un campo

DEF (OMOOMORFISMO DI CAMPI)

Un omoomorfismo di campi $f: K \rightarrow L$ è un caso particolare di omoomorfismo di anelli commutativi.

In altre parole $f: K \rightarrow L$ è un omonom. \Leftrightarrow :

- $f(x+y) = f(x) + f(y)$
- $f(xy) = f(x)f(y)$
- $f(1_K) = 1_L$

PROPOSIZIONE

Un omoomorfismo di campi $f: K \rightarrow L$ è iniettivo.

DIM

$$f(x) = f(y) \Rightarrow f(x-y) = 0_L$$

Se $z = x-y \neq 0 \Rightarrow z^{-1} \exists$, dunque:

$$\begin{aligned}
 1_L &= f(1_K) = f(z z^{-1}) = \underbrace{f(z)}_{=0_L} f(z^{-1}) = 0_L f(z^{-1}) = 0_L \quad \frac{\downarrow}{\cancel{f(z)}} \\
 &\quad \text{perché } z = x-y \\
 &\quad \in f(x-y) = 0
 \end{aligned}$$

NOTA: Un omomorfismo di campi seiettivo è un isomorfismo

DEF (SOTOCAMPO)

Sia L un campo.

Allora un sottoinsieme $K \subseteq L$ si chiama sottocampo se $1 \in K$ e K è chiuso rispetto all'addizione, la moltiplicazione, l'inverso additivo e moltiplicativo di elementi diversi da zero.

ESEMPIO: $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ è una successione di sottocampi

PROPOSIZIONE

- \mathcal{L} è l'immagine di un omomorfismo di campi
 $f: K \rightarrow L$ è un sottocampo di L .
- \mathcal{L} l'intersezione di due sottocampi di K è anch'essa un sottocampo di K .

DIM

- $\text{Im}(f) = \{f(x) : x \in K\}$
 - $f(1_K) = 1_L \in \text{Im}(f)$
 - $a = f(\alpha), b = f(\beta) \in \text{Im}(f)$
 $\Rightarrow ab = f(\alpha)f(\beta) = f(\alpha\beta) \in \text{Im}(f)$
 - $a = f(\alpha), b = f(\beta) \in \text{Im}(f)$
 $\Rightarrow a+b = f(\alpha)+f(\beta) = f(\alpha+\beta) \in \text{Im}(f)$
 - $a = f(\alpha), a \neq 0 \Rightarrow \exists a^{-1} \in \text{Im}(f) \text{ t.c. } a^{-1}a = aa^{-1} = 1_K$
 - $a = f(\alpha), a \neq 0 \Rightarrow \exists a' \in \text{Im}(f) \text{ t.c. } a'+a = a+a' = 0_K$

- Sia $S = \bigcap F_i$, F_i sottocampi di K

- $0, 1 \in F_i \forall i \Rightarrow 0, 1 \in S$
- $\forall a \neq 0 \in F_i \exists a^{-1} \in F_i \text{ t.c. } aa^{-1} = a^{-1}a = 1_{F_i} \Rightarrow a^{-1} \in S$

- $\forall a \neq 0 \in F; \exists a' \in F; \text{ c. } a+a'=a'+a=0_F \Rightarrow a' \in S$
- $a, b \in F \Rightarrow ab \in F \Rightarrow ab \in S$
- $a, b \in F \Rightarrow a+b \in F \Rightarrow a+b \in S$

D

DEF (SOTOCAMPPO OTENUTO ANNETTENDO S A K)

Sia K un sottocampo di L e S un sottoinsieme di L . Allora l'intersezione di tutti i sottocampi di L che contengono K e S è il sottocampo $K(S)$ di L e si chiama sottocampo ottenuto ammettendo S a K .

$$K(S) = \bigcap_{\substack{K' \subseteq L \\ \text{sottocampo} \\ S \subseteq K'}} K'$$

ESEMPIO

$$\underline{Q(\sqrt{2}) \subseteq \mathbb{R} = \{a+b\sqrt{2} : a, b \in Q\}}$$

↳ campo ottenuto ammettendo $\sqrt{2}$ a Q

- $a+b\sqrt{2} + c+d\sqrt{2} = (a+c) + (b+d)\sqrt{2} \Rightarrow$ CHIUSO PER ADD.
- $(a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2bd) + \sqrt{2}(ad+bc) \Rightarrow$ CHIUSO PER MUL.
- $\frac{1}{a+b\sqrt{2}} \cdot \frac{a-b\sqrt{2}}{a-b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2}$

ma $a^2 - 2b^2 = 0$ non ha sol. per $a, b \in Q$

DEF (SOTOCAMPPO PRIMO)

Il sottocampo primo F di K è l'intersezione di tutti i sottocampi primi di K .

LEMMA

Il sottocampo primo \mathbb{F} di k è isomorfo a \mathbb{Q} o a \mathbb{Z}_p per qualche numero primo p .

DIM

Sia $f: (\mathbb{Z}, +) \rightarrow (k, +)$ l'omomorfismo di gruppi t.c. $f(1_{\mathbb{Z}}) = 1_k$.

Supponiamo $\ker(f) \neq 0$.

Allora, sia n il più piccolo intero positivo t.c. $f(n) = 0$.

Se n non è primo, scriviamo $n = ab$ con $a, b > 1$.

Allora $f(a)f(b) = f(ab) = 0 \Rightarrow \underbrace{f(a) = 0}_{\downarrow} \text{ oppure } f(b) = 0 \uparrow$

$$\Rightarrow \text{Im}(f) \cong \mathbb{Z}/p\mathbb{Z}$$

Se f è iniettiva, allora $\phi(a/b) = f(a)/f(b)$ è un omomorfismo da \mathbb{Q} a k .

$\Rightarrow \phi(\mathbb{Q})$ è un sottocampo isomorfo a \mathbb{Q}

□

CARATTERISTICA DI UN CAMPO

Se il campo primo di k è \mathbb{Z}_p , diciamo che k ha caratteristica p ($\text{char}(k) = p$).

Altrimenti, diciamo che $\text{char}(k) = 0$.

SPAZIO VETTORIALE SU UN CAMPO k

Sia k un campo. Allora uno spazio vett. sul campo k è un insieme V dotato di due operazioni:

- $k \times V \rightarrow V$, $(c, v) \mapsto cv$ (MOLTIPLICAZIONE)
- $V \times V \rightarrow V$, $(v, w) \mapsto v+w$ (ADDITIONE VETTORE)

che soddisfano i soliti assiomi di uno spazio vett.

Valgono, in generale, tutti gli aspetti dell'algebra lin. che non coinvolgono prodotti scalari (in quanto ad es. \mathbb{Z}_p non è un campo ordinato come lo è \mathbb{R}).

Se U e V sono spazi vett. su un campo K di dim. finita e $\dim U = \dim V$, allora U e V sono isomorfi come spazi vett.

LEMMA

Se K è un sottocampo di L , allora L è uno spazio vett. su K rispetto alle operazioni:

- $(x, y) \in L \times L \mapsto x + y$ (ADD. IN L)
- $(c, x) \in K \times L \mapsto cx$ (MULT. IN L)

In questo caso diciamo che L è un'estensione di K e scriviamo $L:K$

DIM

$$K \times L \rightarrow L$$

- i) $l_1 + l_2 = l_2 + l_1$,
- ii) $(l_1 + l_2) + l_3 = l_1 + (l_2 + l_3)$
- iii) $0 + l = l + 0 = l$
- iv) $l + (-l) = 0$

$(L, +)$ è un gruppo abeliano perché L è un campo
 \Rightarrow gli assiomi relativi all'addizione sono verificati

- v) $(k_1 k_2)l = k_1(k_2 l)$
- vi) $(k_1 + k_2)l = k_1l + k_2l$
- vii) $k(l_1 + l_2) = kl_1 + kl_2$
- viii) $1l = l$

Gli assiomi relativi alla moltiplicazione sono tutti verificati perché K è un sottocampo di L
 $(\Rightarrow K$ è un campo $\Rightarrow K$ è un anello comm. con id.)



Se K è un sottocampo di L , indichiamo con $[L:K]$ la dim. di L come spazio vett. su K .

$[L:K] < \infty \Rightarrow L$ è un'estensione finita di K

DEF (ELEMENTO ALGEBRICO)

Sia L un'estensione di un campo K .

Allora, $\alpha \in L$ si dice essere algebrico su K se esiste un polinomio non costante $f(t) \in K[t]$ t.c. $f(\alpha) = 0$.

LEMMA

Se L è un'estensione del campo K e $[L:K] < \infty$, allora ogni elemento $\alpha \in L$ è algebrico su K .

DIM

Siamo $\alpha \in L$, $[L:K] = n$

$\Rightarrow \{1, \alpha, \dots, \alpha^n\}$ non possono essere lin. indip.
(perché $|\{1, \alpha, \dots, \alpha^n\}| = n+1 > [L:K]$)

$$\Rightarrow f(x) = \sum_{j=0}^n c_j x^j, \quad f(\alpha) = 0$$

□

DEF (POLINOMIO IRONICO DI GRADO MINIMO)

Sia L un'estensione di K e supponiamo che $\alpha \in L$ sia algebrico su K .

Allora, il polinomio minimo $m = m_\alpha$ di α è il polinomio monico di grado minimo in $K[t]$ t.c. $m(\alpha) = 0$.

(m_α è unico)

DEF (TORE DI ESTENSIONI DI CAMPI)

Siamo $L:K$ e $M:L$ estensioni di campi.

Allora $M:K$ (K è un'estensione di K).

In questo caso diciamo che $K \subseteq L \subseteq M$ è una torre di estensioni di campi.

TH (LEGGE DELLA TORRE)

Sia $K \subseteq L \subseteq M$ una torre di estensioni di campi.
Se $[M:L] < \infty$, $[L:K] < \infty$, allora $[M:K] < \infty$ e
 $[M:K] = [M:L][L:K]$.

DIM

Siamo $[M:L] = m$, $[L:K] = l$

Sia $\{\alpha_1, \dots, \alpha_m\}$ una base per M su L

Sia $\{\beta_1, \dots, \beta_l\}$ " " " L su K

i) Dobbiamo dim. che $B = \{\alpha_i \beta_j : 1 \leq i \leq m, 1 \leq j \leq l\}$
è una base per M su K :

$$\mu \in M \Rightarrow \mu = \sum_{i=1}^m \alpha_i \alpha_i, \quad \alpha_1, \dots, \alpha_m \in L$$

$$\text{In particolare } \alpha_i = \sum_{j=1}^l b_{ij} \beta_j, \quad b_{i1}, \dots, b_{il} \in K$$

$$\therefore \mu = \sum_{i=1}^m \alpha_i \alpha_i = \sum_{i=1}^m \left(\sum_{j=1}^l b_{ij} \beta_j \right) \alpha_i = \sum_{i=1}^m \sum_{j=1}^l b_{ij} \beta_j \alpha_i$$

$$\Rightarrow M = \text{span}_K(B)$$

ii) Ora dobbiamo dim. che B è linearmente indipendente

$$\text{Supp. } \sum_{i=1}^m \sum_{j=1}^l b_{ij} \beta_j \alpha_i = 0, \text{ allora } \sum_{i=1}^m \left(\sum_{j=1}^l b_{ij} \beta_j \right) \alpha_i = 0$$

Allora, poiché $\{\alpha_1, \dots, \alpha_m\}$ è lin. indip., $\sum_{j=1}^l b_{ij} \beta_j = 0$
Poiché $\{\beta_1, \dots, \beta_l\}$ è lin. indip., $b_{ij} = 0 \quad \forall i, j$
 $\therefore B$ è lin. indip.

$$\therefore [M:K] = |B| = ml = [M:L][L:K]$$

□

PROPOSIZIONE

Sia K un campo con sottocampo primo \mathbb{F} .

Se K contiene un numero finito di elementi allora $\text{char}(K) = p$ per qualche numero primo p e $|K| = p^n$ dove n è la dimensione di K su \mathbb{F} ($n = [K : \mathbb{F}]$) -

DIM

$\text{char}(K) = 0 \Rightarrow K$ ha un sottocampo isomorfo a \mathbb{Q} e quindi $|K| = \infty$

$\text{char}(K) = p$

$[K : \mathbb{F}] = \infty \Rightarrow K$ contiene un insieme infinito di elem. lin. indipendenti

$$\therefore [K : \mathbb{F}] < \infty$$

\Rightarrow come spazio vett. $K \cong \mathbb{F}^n$

$$\Rightarrow |K| = |\mathbb{F}^n| = p^n$$

□

NOTA: a meno di isomorfismi, c'è un solo campo di ordine p^n

DEF

Sia $\mathbb{R}^{\mathbb{N}}$ l'insieme di tutte le funzioni $\mathbb{N} \rightarrow \mathbb{R}$ dare

$$\mathbb{N} = \{0, 1, \dots\}$$

Dato $f \in \mathbb{R}^{\mathbb{N}}$ sia $\text{supp}(f) = \{x \in \mathbb{N} : f(x) \neq 0\}$ -

Allora $\mathbb{R}[x] = \{f \in \mathbb{R}^{\mathbb{N}} : |\text{supp}(f)| < \infty\} =$ insieme dei polim. nella var. x con coeff. nello stesso \mathbb{R}

La notazione convenzionale è:

$$f \in \mathbb{R}[x] \subset \mathbb{R}^{\mathbb{N}} \longleftrightarrow \sum_k f(k) x^k$$

dove la sommatoria ha un num. finito di termini -

LEMMA

Sia L un'estensione del campo K e sia $\alpha \in L$ un elemento algebrico.

Allora, il polinomio minimo $m \in K[t]$ di α è irriducibile.

DIM

Supponiamo $m = fg$ con f, g polinomi non costanti.

Allora, poiché $K[t]$ è un dominio di integrità:

$$0 = m(\alpha) = f(\alpha)g(\alpha) \Rightarrow f(\alpha) = 0 \text{ oppure } g(\alpha) = 0$$

Che contraddice la minimialità del grado di m .

LEMMA

Sia L un'estensione del campo K e $\alpha \in L$ un elem. algebrico con polinomio minimo m .

Supponiamo che $f \in K[t]$ sia un polinomio monico irriducibile t.c. $f(\alpha) = 0$.

Allora $f = m$.

DIM

$$m = m_\alpha \Rightarrow f = qm + r \text{ dove } r = 0 \text{ oppure } \deg(r) < \deg(m)$$

$$\Rightarrow 0 = f(\alpha) = \underbrace{q(\alpha)m(\alpha)}_{=0} + r(\alpha) = r(\alpha)$$

$r \neq 0$ contraddice la minimialità del grado di m

$r = 0$ contraddice l'irriducibilità di f , a meno che q non sia un polinomio costante

$$f, m \text{ monici} \Rightarrow q = 1$$

□

PROPOSIZIONE

Sia α è algebrico su K con polinomio minimo m di grado d allora $\{1, \alpha, \dots, \alpha^{d-1}\}$ sono lin. indipendenti. (se $\alpha \in K$ questo insieme è solo $\{1\}$)

DIM

Supponiamo che $\sum_{k=0}^{d-1} c_k \alpha^k = 0$ sia una relazione di dipendenza lineare (non banale, quindi $c_0, \dots, c_d \neq 0$). Allora, $f(t) = \sum_{k=0}^{d-1} c_k t^k$ è un polinomio non costante che annulla α .

Dopo avere riscalato, possiamo supporre che f sia un polinomio monico di grado minore di $d = \deg(m)$ t.c. $f(\alpha) = 0$, che contraddice la minimalità di m . □

PROPOSIZIONE

Sia $\alpha \in L$ algebrico su K con polinomio minimo di grado d e $W = \text{span}_K \{1, \alpha, \dots, \alpha^{d-1}\}$.

Quindi $K(\alpha) = W$.

DIM (vedi meglio dispensa)

W è un sottocampo di L che contiene $\alpha \in K$.

Quindi, $K(\alpha) \subseteq W$ perché $K(\alpha)$ è il sottocampo più piccolo di L che contiene $\alpha \in K$.

Infine $W \subseteq K(\alpha)$ perché dato che $K(\alpha)$ è un campo contenente K e α , deve contenere tutte le comb. lineari di $1, \alpha, \dots, \alpha^{d-1}$. □

NOTA (sull'irriducibilità dei polinomi):

$$f = gh \quad g, h \in \mathbb{Z}[x]$$

$$\Rightarrow [f] = [g][h] \text{ in } \mathbb{Z}_p[x], p \text{ primo}$$

$$\therefore [f] \in \mathbb{Z}_p[x] \text{ irriducibile} \Rightarrow f \in \mathbb{Z}[x] \text{ irriducibile}$$

Ora: se f è irreducibile modolo un primo qualunque, allora è irreducibile anche in $\mathbb{Z}[x]$.

ES

$$f(x) = x^3 + x + 1$$

$f(x)$ è irreducibile in $\mathbb{Z}_2[x]$ perché $f(x) \neq 0 \forall x$:

$$f(0) = 1 \pmod{2}$$

$$f(1) = 3 \pmod{2}$$

$\Rightarrow f(x)$ è irreducibile in $\mathbb{Z}[x]$